This project that has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020 SU-FCT-2019, under grant agreement no 883341.

Global Response Against Child Exploitation

Instrument: Research and Innovation Action proposal

Thematic Priority: FCT-02-2019

Legal Report v2

Deliverable number	D9.4	
Version:	2.1	
Delivery due date:	31 July 2023	
Dissemination level:	PU	
Classification level:	Non classified	
Status	Final	
Nature:	Report	
Main author(s):	Ulrich Gasper Prof. Dr. Marco Gercke Gunhild Scheer	CRI CRI CRI
Contributor(s):	Anton Toni Klančnik, MA (section 2.4.1 and chapter 13) Thalia Prastitou (section 2.4.2 and chapter 14) Pedro Vicente (section 2.4.3 and chapter 15) Sigute Stankeviciute (section 2.4.5 and chapter 17)	Europol EUC PJ L3CE

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
1.0	31/05/2021	Ulrich Gasper, Prof. Dr. Marco Gercke, Gunhild Scheer, Thalia Prastitou, Pedro Vicente, Sigute Stankeviciute	Submission of v1 of this document: D9.3 – Legal Report v1
1.1	08/07/2022	Ulrich Gasper (CRI)	Initial draft v2
1.2	04/01/2023	Thalia Prastitou (EUC)	Bilateral Agreements in Cyprus
1.3	11/01/2023	Sigute Stankeviciute (L3CE)	Bilateral Agreements in Lithuania
1.4	28/01/2023	Pedro Vicente (PJ)	Bilateral Agreements in Portugal
1.5	14/03/2023	Anton Toni Klančnik, MA (Europol)	Bilateral Agreements in Slovenia
1.6	04/07/2023	Anton Toni Klančnik, MA (Europol)	Country Report on Slovenia
1.7	13/07/2023	Ulrich Gasper (CRI)	Final draft v2
1.8	24/07/2023	Carla Costa (PJ)	Peer Review
1.9	25/07/2023	Ulrich Gasper (CRI)	Incorporation of Peer Review
1.9	28/07/2023	Jonathan Middleton (SAB)	SAB assessment with no classification required
2.0	28/07/2023	Peter Leskovsky	Final check before submission.
2.0	18/08/2023	Anton Toni Klančnik, MA (Europol), Panagiotis Daousis Ntres (Europol)	Peer Review
2.1	22/08/2023	Ulrich Gasper (CRI)	Incorporation of Peer Review
2.1	24/08/2023	Peter Leskovsky	Re-submission after minor changes

DISCLAIMER

Every effort has been made to ensure that all statements and information contained herein are accurate; however, the Partners accept no liability for any error or omission in the same.

This document reflects only the view of its authors and the European Commission is not responsible for any use that may be made of the information it contains.

Executive Summary

This Deliverable D9.4 presents the legal framework relevant not only for the activities in the course of the GRACE project but also for the use of the GRACE tools and platform after a potential roll-out of the GRACE solution. This legal framework consists of a complex interplay between international and national layers of rules and regulations. *Chapter 1* introduces the methodology applied and approach chosen for Deliverable D9.4 and provides an overview of its contents as well as its function in relation to other deliverables.

The first part of this Deliverable D9.4 comprises chapters 2.–12. which are dedicated to the analysis of the international legal frameworks consisting of the relevant international treaties at global level of the United Nations as well as at regional level of the Council of Europe. Further, the available rules and regulations at supranational level of the European Union are examined in the following seven key areas of interest:

- *Chapter 2* provides an overview and analysis of the legal instruments at international and regional level related to cross border cooperation and cross-border exchange of court-proof evidence.
- *Chapter 3* provides a brief overview of the international standards which are built on the global consensus that the harm of CSEM is so substantial, that it requires extensive criminalization. This overview is vital background information for all researchers participating in the GRACE project on the reasons why there are highly complex processes in place preventing any researcher from access to CSEM.
- *Chapter 4* takes a closer look at the regulatory framework on preventing and combating online child sexual abuse (CSA) proposed by the European Commission in May 2022 and provides a first analysis how this future regulatory framework may affect to the tools and platform developed in the course of the GRACE project.
- *Chapter 5* takes a closer look at the regulatory framework for artificial intelligence proposed by the European Commission in April 2021 as well as the amendments suggested by the Council and the European Parliament and provides a first analysis how this future regulatory framework will apply to the tools and platform developed in the course of the GRACE project.
- *Chapter 6* provides an overview of the legal frameworks established in international treaties at global level by the United Nations and at regional level by the Council of Europe as well as of the legal framework for victims' rights within the European Union.
- *Chapter 7* provides an overview of the relevant legal framework for data protection at European level for two phases regarding the GRACE project: First there is the *research phase* during which the GRACE tools and platform are developed as prototype and second there is the *after-roll-out phase* when the GRACE tools and platform are potentially put to use by LEAs in their fight against CSEM. For each phase, two separate and overlapping legal regimes governing the protection of personal data emanating from the right to respect for private and family life enshrined in the European Convention on Human Rights (ECHR), on the one side, and the Charter of Fundamental Rights of the European Union (Charter of Fundamental Rights), on the other.
- *Chapter 8* presents the key challenges for electronic data as criminal evidence because the online dimension of CSE is intrinsically tied to electronic data. Further, this chapter takes a brief look at the most recent proposals aiming to overcome the lack of legal frameworks for electronic evidence in criminal investigations and proceedings in international treaties at global level by the United Nations and at regional level by the Council of Europe as well as at the proposal for electronic evidence within

the European Union. Finally, this chapter highlights an approach for classifying electronic evidence which has been developed by *Warken* based on the affected data subject's fundamental rights.

- *Chapter 9* takes a look at existing databases for CSEM available to law enforcement and considers the fragmentation resulting from the lack of a harmonized legal framework for national CSEM databases or for establishing a centralized EU database.
- *Chapter 10* provides an overview of some of the most relevant areas of law potentially triggered in the course of the legal evaluation of a LEA's authorization to use crawlers as intended by the GRACE solution.
- *Chapter 11* takes a closer look at how the Draft Cyber Resilience Act proposed by the European Commission might affect the GRACE system.
- *Chapter 12* recommendations are contemplated and formulated in an effort to support the definition of potential future standard protocols, procedures and data formats for international, cross-border approved, information exchange and court proof-evidence.

The second part of this Deliverable D9.4 comprises of chapters 13.–17. which outline the national legal framework in Slovenia, Cyprus, Portugal, Germany and Lithuania regarding victims' rights, data protection within the law enforcement ecosystem, the collection and preservation of electronic evidence, the use of image databases and crawlers. While the areas of victims' rights and data protection benefit from detailed guidance of international treaties at global (United Nations) and regional (Council of Europe) level as well as of rules and regulations at supranational level (European Union), the remaining three areas do not enjoy such helpful guidance and consensus so that law enforcement has to rely solely on national rules.

Table of Contents

1. Introduction

The focus of the GRACE project is to improve the ability of law enforcement agencies (LEA) to handle child sexual abuse and exploitation material (CSEM).[1] Fighting against the dissemination of CSEM and the underlying crimes committed against children is a priority at all levels of society, especially for the United Nations/International Community,[2] for each EU Member State as well as for the EU Commission.[3] While contributing to the global efforts in fighting against child sexual abuse and exploitation (CSE), undoubtfully one of the most serious crimes with life-long consequence for victims[4], it is vitally important for the GRACE project to recognize that any solution developed as support for LEAs must fully comply with the applicable legal framework. In the context of the GRACE project there are various legal issues that need to be reflected – including data protection issues and requirements of admissibility of electronic evidence.

Update for Legal Report v2:

In the context of the GRACE project there is a plethora of legal issues gaining significant momentum by the recent increase in the development of specific legislative measures dedicated to enhancing the society's fight against cybercrime in general and against CSE including dissemination of CSEM in particular. Therefore, the decision to assess the legal framework in two sequenced Legal Reports with more than two years in between allows to analyse how this continuous evolution affects the tools and platform developed in the course of the GRACE project. The first Legal Report was submitted as Deliverable D9.3 in May 2021 and this Deliverable D9.4 updates and supplements the Legal Report of Work Package WP9.

1.1. Methodology

The GRACE project aims to ensure that the solution developed as support for LEAs will enjoy full legal compliance and does not implement any operations that could conflict with the requirements of law – especially in an area as sensitive as CSEM. In this respect, the GRACE project needs to recognise that the chances of ensuring such full compliance for a solution potentially used by LEAs in all 27 Member States are limited in areas where there is a high degree of fragmentation in law. In other words: Given the fact that resources for the development of the GRACE solutions are not unlimited, the focus of ensuring legal compliance will be related to areas where either the European Union has undertaken approaches to harmonise legislation or countries are – independently from centralised harmonisation initiative – sufficiently aligned anyway because they have separately implemented comparable legislation. In areas with significant

[1] For more information about the GRACE project, the scope and funding see: https://cordis.europa.eu/project/id/883341

[2] The UN Universal Declaration of Human Rights, that prevents against abuse applies to children: United Nations, General Assembly, Universal Declaration of Human Rights (UDHR), Resolution 217 A, A/RES/3/217 A, 10 December 1948. In addition, the UN Convention on the Rights of the Child addresses specific issues: United Nations, Convention on the Rights of the Child (CRC), Resolution 44/25, adopted on 20 November 1989, entered into force on 2 September 1990.

[3] See in this regard for example the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Strategy for a more effective fight against child sexual abuse, COM (2020), 607.

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Strategy for a more effective fight against child sexual abuse, COM (2020), 607, page 1.

fragmentation, ensuring legal compliance will remain the sole responsibility of the LEAs utilizing the solution.

In order to differentiate between areas of law with sufficient common ground because either harmonization has taken place or similar standards exist, on the one hand, and the areas of law with a higher degree of fragmentation, Task T9.2 undertook a two-fold approach: After identifying the areas of relevance for the development of the GRACE solutions, both the availability of international or European standards as well as the national rules and regulations were analysed. Four examples for the complexity of national rules and regulations are provided in the country reports on Cyprus (chapter 9. below), Portugal (chapter 10. below), Germany (chapter 11. below) and Lithuania (chapter 12. below). It is important to underline that the intention of including these country-specific analyses is not to offer a complete in-depth documentation of the rules and regulations in each country, but rather to demonstrate sufficient information for the evaluation whether there is fragmentation among national framework.

1.2. Overview

The DoA describes this Deliverable as:

> *D9.3 – This deliverable will summarize the legal environment and define the potential legal concerns related to use of Big Data, Machine Learning and AI with regard to investigations concerning child sexual exploitation and abuse material (CSEM). [M12]*

This Deliverable D9.3 has two main objectives: The *first* main objective is to identify potential (harmonized) legal frameworks that are relevant for the application of the GRACE solution. Such relevance has repercussions on the design process because some legal frameworks may require the limitation of specific functions for the GRACE tools and platform. The GRACE Consortium is fully committed to the concept of "legal compliance by design". The *second* main objective is the identification of areas where researchers participating in the development of the GRACE tools and platform need to be particularly wary of infringing the legal framework.

It is important to emphasise that the purpose of this Deliverable is not to determine whether a LEA in one of the 27 EU Member States will be authorized to carry out investigations using the GRACE solution or whether evidence collected and/or processed by using the GRACE solution will be admissible in court. These important questions will require a case-by-case evaluation by each institution that plans to utilize the GRACE solution.

Update for Legal Report v2:

The DoA describes the Task relevant for both Legal Reports of Work Package WP9 as:

> "T9.2 – Assessment of legislation covering LEA use of Big Data and AI [M0-33]
>
> *The focus of this task will be on an assessment of relevant legal standards.*
>
> *The starting point will be global and European (EU as well as Council of Europe) standards. In addition, the legislation of selected Member States will be analysed; this will, at least, include the 5 countries. Consortium Members from different countries will provide at least one sub-chapter, providing input with regard to the collection of issues as well as literature review for the creation of an inventory. Consortium members from the different countries will support the collection of relevant national legislation and draft a national chapter. CRI will co-ordinate the work and carry out the comparative analysis.*
>
> *Also, in this task, the analysis of legal issues related to cross-border exchange of court-proof evidence will be tackled. In a first step legal instruments related to cross border cooperation and cross-border exchange will be collected and analysed. This shall include regional (especially EU and CoE*

instruments), international (especially UNTOC) and bi-lateral agreements. In a second step the requirements (both technical and legal) for court-proof evidence in up to 5 countries will be collected and analysed.

Based on the results of the analysis recommendations will be formulated to support the definition of standards protocols, procedures and data formats for international, cross-border approved, information exchange and court proof-evidence. D9.3 will include as annex a report on legal issues related to cross-border investigations. "

This Deliverable D9.4 updates and supplements the first Legal Report of Work Package WP9 submitted as Deliverable D9.3. The first Legal Report (Deliverable D9.3) identified not only potential legal frameworks that are relevant for the application of the GRACE solution and have repercussions on the design process of specific functions for the GRACE tools and platform, but also areas where researchers participating in the development of the GRACE tools and platform need to be particularly wary of infringing the legal framework.

This second Legal Report (Deliverable D9.4) continues the two-fold approach selected for Task T9.2 distinguishing between areas of law with sufficient common ground and the areas of law with a higher degree of fragmentation. While both, the availability of international or European standards as well as the national rules and regulations in Cyprus (chapter 14. of D9.3), Portugal (chapter 15. of D9.3), Germany (chapter 16. of D9.3) and Lithuania (chapter 17. of D9.3) have been analysed in the first Legal Report, the fifth example illustrating the complexity of national rules and regulations is provided in the country report on Slovenia (chapter 13. below). These 5 country-specific analyses are not intended to offer a comprehensive in-depth documentation of the national rules and regulations. Rather, the intention for including country reports of 5 selected Member States in the Legal Report of Work Package WP9 is to demonstrate sufficient information for the evaluation whether and in which areas there is fragmentation among national frameworks.

In line with the description of the task in the Grant Agreement, this Deliverable D9.4 completes the Legal Report by providing an overview as well as an analysis of the legal instruments related to cross border cooperation and cross-border exchange of court-proof evidence (chapter 2. below). This new chapter on international cooperation also includes a brief overview of selected bilateral agreements concluded by each of the 5 Member States selected for the country reports in the Legal Report of Work Package WP9 (section 2.4 below) which expands and complements the distinction among areas of law between sufficient common ground and significant fragmentation.

1.3. Selection of Areas of Law / Red Teaming Exercise

For the purposes of focus control, Task T9.2 included a red teaming exercise to identify legal concerns that need to be included in the assessment provided in this Deliverable D9.3.

Red teaming or alternative analysis is a specific method used to review plans, strategies, and hypotheses.[5] Two

[5] See: *Herman/Frost/ Kurz*, Wargaming for Leaders. 2009; *Sabin*, Simulating War, 2012; Fryer-Biggs, Building better cyber red teams, defensenews.com, 14 June 2012; *Lauder*, Red Dawn: The Emergence of a red teaming capability in the Canadian Forces, Canadian Army Journal, Vol. 12.2, 2009; *Longbine*, Red Teaming: Past and Present, 2008; *Wood/Duggan*, Red Teaming of Advanced Information Assurance Concepts, DARPA Information Survivability Conference and Exposition, 2002. DISCEX 00 Proceedings, Vol. 2, S. 112ff.

teams are formed, a Red Team and a Blue Team.[6] The Red Team assumes the role of the attacker, while the Blue Team focuses on defense.[7] This method has been successfully employed by the military for decades[8] and has also been applied in civil activities for a number of years.[9] It is explicitly not restricted to acting out physical attacks. The methodology can also be used to investigate theoretical issues from different angles and with varying emphases – reaching as far as intangible constructs such as a legislative draft.[10] Red teaming can be particularly useful when developing cybersecurity strategies, since the attack situation reflects the real threat situation. However, strategies are mostly developed from the defense angle. A change or expansion of perspective enables a company's own strategies to be examined more critically. Red teaming is not limited to military context, but it can even be utilized in the process of drafting legislation. [11] CRI, the task leader for T9.2, successfully has utilized this approach in several other EU-funded projects. The red teaming exercise revealed potential legal conflicts related to the use of CSEM databases, AI as well as the utilization of crawlers. As a consequence, these topics were included in the list of legal topics selected for analysis.

The completed list included the following topics:

- Legislation related to Artificial Intelligence (chapter 3. of D9.3, now 5. below),
- Legislation related to Victim' Rights (chapter 4. of D9.3, now 6. below),
- Legislation related to Data Protection (chapter 5. of D9.3, now 7. below),
- Legislation related to Electronic Evidence (chapter 6. of D9.3, now 8. below),
- Legislation related to CSEM Image Databases (chapter 7. of D9.3, now 9. below),
- Legislation related to Crawlers (chapter 8. of D9.3, now 10. below),
- Legislation related to Cross Border Cooperation (chapter 2. below),

With regard to the complexity of the issue of cross border cooperation and in line with the description of the task in the Grant Agreement the issue of cross border access and especially the development of recommendations will be tackled after the submission of this Deliverable D9.3 and included in Deliverable D9.4.

Update for Legal Report v2:

After submission of the first Legal Report in May 2021, various new legislative measures have either been proposed or set in motion for the elaboration of a proposal dedicated to enhancing the society's fight against

[6] See *Wood/Duggan*, Red Teaming of Advanced Information Assurance Concepts, DARPA Information Survivability Conference and Exposition, 2002. DISCEX 00 Proceedings, Vol. 2.

[7] See *Meija*, Red Team Versus Blue Team – How to run an effective Simulation, CSO 25.03.2008.

[8] See *Lauder*, Red Dawn: The Emergence of a red teaming capability in the Canadian Forces, Canadian Army Journal, Vol. 12.2, 2009; *Longbine*, Red Teaming: Past and Present, 2008.

[9] See *Lauder*, Red Dawn: The Emergence of a red teaming capability in the Canadian Forces, Canadian Army Journal, Vol. 12.2, 2009.

[10] See *Gercke*, "Red Teaming" Ansätze zur Effektivierung von Gesetzgebungsprozessen? Die Übertragbarkeit einer klassischen, militärischen Methodik auf Gesetzgebungsprozesse im IT-Bereich, CR 2014, page 344 et seq.

[11] See *Gercke*, "Red Teaming" Ansätze zur Effektivierung von Gesetzgebungsprozessen? Die Übertragbarkeit einer klassischen, militärischen Methodik auf Gesetzgebungsprozesse im IT-Bereich, CR 2014, page 344 et seq.

cybercrime in general and against CSE including dissemination of CSEM in particular:

- UN Ad Hoc Committee elaborating "convention on countering the use of information and communications technologies for criminal purposes"
- EU Amended Europol Regulation
- EU Draft Police Cooperation Code:
  - Draft Prüm II Regulation
  - Draft Information Exchange Directive
- EU Draft Regulation laying down rules to prevent and combat child sexual abuse

In addition to these new legislative measures, the legislative proposals mentioned in the first Legal Report have continued to evolve significantly so that a fresh assessment is appropriate:

- CoE Second Additional Protocol to Budapest Convention
- EU Artificial Intelligence Act
- EU Draft eEvidence Package

Against the background of these new legislative developments, Task T9.2 included a second red teaming exercise to identify emerging legal concerns that need to be included in the updated and supplemented assessment provided in this Deliverable D9.4. This second red teaming exercise revealed a significant shift of potential legal conflicts related to the use of CSEM databases, AI as well as the utilisation of crawlers. As a consequence, the complete list of relevant legal areas identified for this second Legal Report comprises the following topics:

- Legislation related to Cross-Border Cooperation (chapter 2. below),
- Legislation related to Criminalisation of CSEM (chapter 3. below),
- Legislation related to the Fight Against Online CSA (chapter 4. below),
- Legislation related to Artificial Intelligence (updated in chapter 5. below),
- Legislation related to Victim' Rights (updated chapter 6. below),
- Legislation related to Data Protection (updated in chapter 7. below),
- Legislation related to Electronic Evidence (updated in chapter 8. below),
- Legislation related to CSEM Image Databases (updated in chapter 9. below),
- Legislation related to Crawlers (updated in chapter 10. below),
- Legislation related to Cyber Resilience (chapter 11. below),

Against the background of this legal analysis, recommendations are contemplated and formulated in an effort to support the definition of potential future standard protocols, procedures and data formats for international, cross-border approved, information exchange and court proof-evidence (chapter 12. below).

1.4. Relation to Other Deliverables

This deliverable is related to the following other GRACE deliverables:

Receives inputs from:

Deliv. #	Deliverable title	How the two deliverables are related
D1.3	Data Management Plan	Both cover data protection issues
D1.4	SELP Guidelines	Both address similar topics – however with D1.4 focusing on practical aspects of the research
WP2 deliverables	DESIGN - Use Cases, Requirements, Standardisation, Technical and Architecture Specification, Security and Auditing	Deliverables submitted in WP2 so far have tried to design the first version of GRACE platform in compliance with legislation.
D9.1	Ethical Report	Some of the Ethical Aspects also have a legal implication
D10.6	Stakeholder and policy recommendations for addressing online CSEM	Links legislation with policy and phenomenon which will help as a guidance for the reader and the designers of the platform

Table 1 – Relation to other deliverables – receives inputs from

Provides outputs to:

Deliv. #	Deliverable title	How the two deliverables are related
D2.2	Use Cases, Process and Data Flows Refinement v2	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D2.3	Use Cases, Process and Data Flows Refinement v3	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D2.5	User requirements v2	General implication of the D9.3 deliverable
D2.11	Technical and Architecture Specifications v2	General implication of the D9.3 deliverable
D2.12	Technical and Architecture Specifications v3	General implication of the D9.3 deliverable
D2.13	Technical and Architecture Specifications v4	General implication of the D9.3 deliverable
D2.15	Security and auditing mechanisms report v2	General implication of the D9.3 deliverable – especially with regard to the security related issues addressed in D9.3
D2.16	Security and auditing mechanisms report v3	General implication of the D9.3 deliverable – especially with regard to the security related issues addressed in D9.3

D2.17	Security and auditing mechanisms report v4	General implication of the D9.3 deliverable – especially with regard to the security related issues addressed in D9.3
D3.2	Data acquisition module v2	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D3.3	Data acquisition module v3	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D3.5	Data pre-processing module v2	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D3.6	Data pre-processing module v3	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D3.8	Data loading and mapping module v2	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D3.9	Data loading and mapping module v3	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D3.11	Content management and digital evidence tamper detection module v2	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D3.12	Content management and digital evidence tamper detection module v3	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D4.11	Digital evidence tamper detection module v2	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D4.12	Digital evidence tamper detection module v3	General implication of the D9.3 deliverable – especially with regard to data protection issues and crawlers
D5.2	Federated data annotation tools	General implication of the D9.3 deliverable – especially with regard to AI
D5.3	Reporto n FEderated Learning strategies	General implication of the D9.3 deliverable – especially with regard to AI
D5.4	Secure data exchange mechanism	General implication of the D9.3 deliverable
D6.1	Module(s) to perform cross-matching and entity mapping between referrals	General implication of the D9.3 deliverable

D6.2	Module(s) to perform content analysis and classification	General implication of the D9.3 deliverable
D6.3	Module(s) to perform content-based geo-location	General implication of the D9.3 deliverable
D6.4	Module(s) to perform analysis of knowledge graphs for evidence data fusion	General implication of the D9.3 deliverable
D6.5	Module(s) to perform prioritisation on OSP referral data	General implication of the D9.3 deliverable
D6.6	Module(s) for predictive analysis of short and long-term trends in CSEM	General implication of the D9.3 deliverable
D7.4	GRACE System v2	General implication of the D9.3 deliverable
D7.5	GRACE System v3	General implication of the D9.3 deliverable
D7.6	GRACE Collaborative Application v1	General implication of the D9.3 deliverable
D7.7	GRACE Collaborative Application v2	General implication of the D9.3 deliverable
D7.8	GRACE Collaborative Application v3	General implication of the D9.3 deliverable
D7.9-D7.14	Technical Validation Report v1 – v6	General implication of the D9.3 deliverable
D9.2	Ethical Report v2	General implication of the D9.3 deliverable
D9.4	Legal Report v2	General implication of the D9.3 deliverable
D9.5	Overall legal and ethical framework v1	General implication of the D9.3 deliverable
D9.7	Architecture for technical safeguards – “security and privacy by design” v1	General implication of the D9.3 deliverable
D9.8	Architecture for technical safeguards – “security and privacy by design” v2	General implication of the D9.3 deliverable
D10.7	Stakeholder and Policy Recommendations for Addressing Online CSEM v2	General implication of the D9.3 deliverable
D10.8	Best Practices on Victim Support for LEA First Responders v1	General implication of the D9.3 deliverable

Table 2 – Relation to other deliverables – provides outputs to

1.5. Structure of the Deliverable

This document includes the following chapters:

- Chapter 2 provides an overview and analysis of the legal instruments at international and regional level related to cross border cooperation and cross-border exchange of court-proof evidence.
- Chapter 3 provides a brief overview of the international standards which are built on the global consensus that the harm of CSEM is so substantial, that it requires extensive criminalization. This overview is vital background information for all researchers participating in the GRACE project on the reasons why there are highly complex processes in place preventing any researcher from access to CSEM.
- *Chapter 4* takes a closer look at the regulatory framework on preventing and combating online child sexual abuse (CSA) proposed by the European Commission in May 2022 and provides a first analysis how this future regulatory framework may affect to the tools and platform developed in the course of the GRACE project.
- Chapter 5 takes a closer look at the regulatory framework for artificial intelligence proposed by the European Commission in April 2021 and provides a first analysis how this future regulatory framework will apply to the tools and platform developed in the course of the GRACE project. Looking a bit closer at the mandatory requirements for high-risk AI system, the emerging differences of the regulatory approach between Commission, Parliament and Council are highlighted.
- Chapter 6 provides an overview of the legal frameworks established in international treaties at global level by the United Nations and at regional level by the Council of Europe as well as of the legal framework for victims' rights within the European Union.
- Chapter 7 provides an overview of the relevant legal framework for data protection at European level for two phases regarding the GRACE project: First there is the *research phase* during which the GRACE tools and platform are developed as prototype and second there is the *after-roll-out phase* when the GRACE tools and platform are potentially put to use by LEAs in their fight against CSEM. For each phase, two separate and overlapping legal regimes governing the protection of personal data emanating from the right to respect for private and family life enshrined in the European Convention on Human Rights (ECHR), on the one side, and the Charter of Fundamental Rights of the European Union (Charter of Fundamental Rights), on the other.
- Chapter 8 presents the key challenges for electronic data as criminal evidence because the online dimension of CSE is intrinsically tied to electronic data. Further, this chapter takes a brief look at the most recent proposals aiming to overcome the lack of legal frameworks for electronic evidence in criminal investigations and proceedings in international treaties at global level by the United Nations and at regional level by the Council of Europe as well as at the proposal for electronic evidence within the European Union. Finally, this chapter highlights an approach for classifying electronic evidence which has been developed by *Warken* based on the affected data subject's fundamental rights.
- Chapter 9 takes a look at existing databases for CSEM available to law enforcement and considers the fragmentation resulting from the lack of a harmonized legal framework for national CSEM databases or for establishing a centralized EU database.
- Chapter 10 provides an overview of some of the most relevant areas of law potentially triggered in the course of the legal evaluation of a LEA's authorization to use crawlers as intended by the GRACE solution.
- Chapter 11 takes a closer look at how the Draft Cyber Resilience Act proposed by the European Commission might affect the GRACE system.
- Chapter 12 recommendations are contemplated and formulated in an effort to support the definition of potential future standard protocols, procedures and data formats for international, cross-border approved, information exchange and court proof-evidence.

- Chapter 13 presents a Country Report on Slovenia outlining relevant national rules and regulations regarding victims' rights, data protection within the law enforcement ecosystem, the collection and preservation of electronic evidence, the use of image databases and crawlers.
- Chapter 14 presents a Country Report on Cyprus outlining relevant national rules and regulations regarding victims' rights, data protection within the law enforcement ecosystem, the collection and preservation of electronic evidence, the use of image databases and crawlers.
- Chapter 15 presents a Country Report on Portugal outlining relevant national rules and regulations regarding victims' rights, data protection within the law enforcement ecosystem, the collection and preservation of electronic evidence, the use of image databases and crawlers.
- Chapter 16 presents a Country Report on Germany outlining relevant national rules and regulations regarding victims' rights, data protection within the law enforcement ecosystem, the collection and preservation of electronic evidence, the use of image databases and crawlers.
- Chapter 17 presents a Country Report on Lithuania outlining relevant national rules and regulations regarding victims' rights, data protection within the law enforcement ecosystem, the collection and preservation of electronic evidence, the use of image databases and crawlers.
- Chapter 18 presents a brief summary and evaluation of this Deliverable D9.4 and points out the workload remaining until the end of the GRACE project.

2. International Cross-Border Cooperation

An invaluable source in the fight against CSEM online originates from the obligatory case reporting of CSEM by social media providers in the USA to the National Center for Missing and Exploited Children (NCMEC)[12] and in Canada to the National Child Exploitation Coordination Centre (NCECC)[13]. Within the EU, electronic service providers may on a voluntary basis detect potential CSEM in their services and refer the detected material to child protection NGOs and LEAs for analysis and investigation.[14] The exponential growth of the number of these CSEM reports discovered by providers themselves or reported to them by their users shows no signs of stabilising, let alone declining.[15] When the NCMEC or the NCECC receives a case report involving foreign jurisdictions, the case report is referred on to the relevant national Law Enforcement Agencies (LEAs) depending on the nationality and location of the child and offender.

The GRACE tools and platform aim to deliver significant operational value to LEAs across Europe in tackling the volume of online CSEM reports. At the moment, LEAs in some EU Member States receive referrals by the NCMEC and NCECC directly (e.g., Austria, France, Germany, Ireland, Italy, Lithuania, Netherlands and Spain) whereas LEAs in other EU Member States receive these referrals by using Europol as gateway (e.g., Belgium, Cyprus, Poland, Portugal and Romania). The high-level analytical GRACE tools made available to LEAs via a Federated Platform aim to transform their investigative capabilities into a synchronised and impactful response to the immense influx of reports.

This chapter addresses the cross-border nature of this area of crime by providing an overview and assessment of the legal frameworks governing both, cross border cooperation as well as cross-border exchange of court-proof evidence for law enforcement purposes at international and at regional level. This chapter first looks at the UN framework and presents an understanding why the United Nations have not (yet) adopted a specific cybercrime convention leaving LEAs to resort to a general UN convention on organised crime (section 2.1. below). Second, the guidance and mechanisms for international cooperation provided in the CoE framework are outlined (section 2.2. below). Finally, the existing as well as the soon-to-be mechanisms for international cooperation within the EU framework (section 2.3. below) as well as on the basis of bilateral agreements and international courtesy (section 2.4. below) are described.

2.1. United Nations Framework

At the United Nations, there is no specific cybercrime convention addressing the need for international cooperation to combat cybercrime and providing effective mechanisms for the necessary cooperation between national LEAs against the global threat of CSE. However, the United Nations have initiated drafting activities in 2021 which may well lead to a future UN convention on cybercrime.

[12] www.missingkids.org/footer/media/keyfacts.
[13] https://www.rcmp-grc.gc.ca/en/online-child-sexual-exploitation.
[14] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, 7 December 2021, p. 28, available at: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021.
[15] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, 7 December 2021, p. 24, available at: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021; Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, 5 October 2020, p. 41, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

2.1.1. Towards A Future UN Convention on Cooperation in Combating Cybercrime

The first Legal Report in Deliverable D9.3[16] mentioned the Draft UN Convention on Cooperation in Combating Cybercrime[17] presented by Russia in 2017 as well as the resolution[18] led by Russia to establish a committee of experts to consider establishing an UN cybercrime treaty and pointed out the strong criticism this Russian Draft had received. In December 2019, the General Assembly set these Russian initiatives somewhat aside and decided to launch a process towards a new international treaty on cybercrime by establishing an open-ended ad hoc intergovernmental committee of experts (Ad Hoc Committee) to elaborate a "comprehensive international convention on countering the use of information and communications technologies for criminal purposes". [19] The draft of a future UN convention on cybercrime is currently scheduled to be provided to the General Assembly at its 78th session, which will begin in September 2023 and conclude in September 2024.[20]

The Ad Hoc Committee's drafting process towards a future UN convention on cybercrime is intended to take into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes and, in particular, "the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime" (Expert Group).[21] However, it is important to note that the Ad Hoc Committee is a subsidiary body of the General Assembly and as such not only separate, but due to its different mandate also independent from the Expert Group which is a subsidiary body of CCPCJ, even though UNODC (another subsidiary body of CCPCJ) serves as Secretariat for the Ad Hoc Committee.[22]

The Ad Hoc Committee was tasked to convene at least six negotiating sessions of 10 days each, held no less

[16] See: section 7.2 below.
[17] See United Nations, General Assembly, Annex to the letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, A/C.3/72/12, 16 October 2017, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/329/59/PDF/N1732959.pdf?OpenElement.
from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General
[18] United Nations, Resolution 73/187, Countering the use of information and communications technologies for criminal purposes, General Assembly, A/RES/73/187, adopted on 17 December 2018, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/53/PDF/N1845053.pdf?OpenElement.
[19] General Assembly, „Countering the use of information and communications technologies for criminal purposes", Resolution 74.247, A/RES/74/247, adopted on 27 December 2019, p. 3 at para. 2, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement.
[20] General Assembly, „Countering the use of information and communications technologies for criminal purposes", Resolution 75.282, A/RES/75/282, adopted on 26 May 2021, p. 2 at para. 4, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement.
[21] General Assembly, Resolution 74.247, A/RES/74/247, adopted on 27 December 2019, p. 3 at para. 2; General Assembly, Resolution 75.282, A/RES/75/282, adopted on 26 May 2021, p. 2 at para. 11.
[22] General Assembly, Resolution 75.282, A/RES/75/282, adopted on 26 May 2021, p. 2 at para. 2.

than 11 weeks apart; and already held five negotiation sessions in March 2022[23], June 2022[24], September 2022[25], January 2023[26], and April 2023[27]. A challenge for all of these negotiating sessions is that any Ad Hoc Committee's decisions on substantive matters without approval by consensus are taken by a two-thirds majority of the representatives present and voting.[28] This development was closely monitored for the GRACE project. Concerning a potential future United Nations standard for international cooperation in combating cybercrime, the current consolidated negotiation document reveals the following five focus areas of the Ad Hoc Committee's sessions regarding potential provisions so far:[29] (1) preamble, (2) international cooperation, (3) preventive measures, (3) technical assistance and (4) the mechanism of implementation and (5) final provisions.

2.1.2. UN Convention Against Transnational Organised Crime (UNTOC)

The main international instrument for judicial cooperation in criminal matters is the United Nations Convention against Transnational Organized Crime (UNTOC).[30] This convention has 190 States parties and with that has achieved almost universal adherence as the only global legally binding instrument to combat

[23] Ad Hoc Committee, Report of First Session, A/AC.291/7, 24 March 2022, available at: https://www.undocs.org/A/AC.291/7. All Documentation of the „First session of the Ad Hoc Committee" in New York, 28 February to 11 March 2022, is available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.
[24] Ad Hoc Committee, Report of Second Session, A/AC.291/10, 27 June 2022, available at: https://www.undocs.org/A/AC.291/10. All documentation of the „Second session of the Ad Hoc Committee", in Vienna, 30 May to 10 June 2022, is available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.
[25] Ad Hoc Committee, Report of Third Session, A/AC.291/14, 28 September 2022, available at: https://www.undocs.org/A/AC.291/14. All Documentation of the „Third session of the Ad Hoc Committee", in New York, 29 August to 9 September 2022, is available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_third_session/main.html.
[26] Ad Hoc Committee, Report of Fourth Session, A/AC.291/17, 2 February 2023, available at: https://www.undocs.org/A/AC.291/17. All Documentation of the „Fourth session of the Ad Hoc Committee", in Vienna, 9 – 20 January 2023, available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html.
[27] Documentation of the „Fifth session of the Ad Hoc Committee", in Vienna, 11 – 21 April 2023, available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main.
[28] General Assembly, Resolution 75.282, A/RES/75/282, adopted on 26 May 2021, p. 2 at para. 5.
[29] Ad Hoc Committee, „ Consolidated negotiating document", A/AC.291/19, 19 December 2022, available at: https://www.undocs.org/A/AC.291/19.
[30] UN Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29 September 2003. UNTOC was supplemented by three protocols, which contain provisions on combating specific forms of organized crime: The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons; the Protocol against the Smuggling of Migrants by Land, Sea and Air, available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-against-smuggling-migrants-land-sea-and-air; and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, available at: https://treaties.un.org/doc/source/RecentTexts/18-12_c_E.pdf.

transnational organized crime and contains important instruments for international cooperation. However, UNTOC was neither specifically designed to address issues related to cybercrime, nor does this convention provide specific provisions dealing with urgent requests for cooperation typically relating to the collection and preservation of data as potential evidence in cybercriminal investigations or court cases.

Nevertheless, this Convention may apply to cybercrimes if the particular crime falls within the scope of application stipulated in Art. 3 UNTOC. According to Art. 3(1) UNTOC, this Convention is only applicable in cybercrime cases if the offence involves an organised crime group. Art. 2 UNTOC defines an organised crime group as a structured group of three or more people. Despite its relevance for cases involving forms of organised crime, UNTOC may not become applicable in cybercrime investigations because cybercrime groups may not be identified as organised crime group. The Internet enables close cooperation with others and coordination of activities without ever having met face-to-face. This makes it feasible for offenders to work together in fluid ad hoc groups.[31]

The procedures for mutual legal assistance are defined in Art. 18 UNTOC which contains the general principles for international cooperation[32] as well as for specific mutual legal assistance requests[33]. The list is complex and ranges from taking evidence to tracing proceeds of crime. In the context of cybercrime investigations, UNTOC does not contain specific wording for data-related requests, such as requests to intercept communication or preserve data. However, Art. 18(3)(i) UNTOC opens the provision to other requests, so UNTOC can also be used for data-related requests.

Art. 18 (4)-(5) UNTOC deal with intelligence sharing stipulating a form of cooperation which takes place on a voluntary basis, without the need for the request.[34] It covers information relating to criminal matters, such as information about potential consumers of CSEM located in another country that has been discovered during an investigation. Especially in complex investigations, where recourse to formal mutual instruments is time-consuming and hence can hinder investigations, LEAs tend to shift to informal means of cooperation. However, information sharing will only be able to work as a substitute if the state receiving the information is able to collect all relevant evidence on its own. In all other cases, formal cooperation is usually required in any event in order to ensure the chain of custody. In the debate on shifting international cooperation from formal requests to spontaneous information sharing, it is necessary to keep in mind that the formal process was developed to protect the integrity of a state as well the rights of the accused. Sharing of information should therefore not circumvent the dogmatic structure of mutual legal assistance.

The procedural aspects of mutual legal assistance are outlined in Art. 18 (6)-(12) UNTOC. In the context of cybercrime investigations, it is important to note that states are enabled to decline mutual assistance requests on the grounds of absence of dual criminality[35] which can hinder international cooperation based on UNTOC.

The form and content of requests as well as the channels of communication are defined in Art. 18 (13)-(16) UNTOC. With regard to channels of communication, UNTOC follows the idea that requests are transmitted

[31] Gercke, „Understanding Cybercrime: phenomena, challenges and legal response“, November 2014, p. 281.
[32] Art. 18(1) and (2) UNTOC.
[33] Art. 18(3) UNTOC.
[34] For details about the intention of the drafters, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, p. 226, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.
[35] Art. 18(9) UNTOC.

from central authority to central authority[36] and emphasises the importance of this procedure to ensure speedy and proper execution of the request. The roles of central authorities may differ, and range from direct involvement in handling and executing requests to forwarding them to the competent authorities. Alternatively, the states have the discretion to require the transmittal through diplomatic channels – a lengthy procedure dramatically slower in transmission and hindering expedited measures such as the preservation of traffic data. While not offering the means of expedited cooperation, UNTOC provides a general procedure for cases of urgency. If states agree, the International Criminal Police Organisation (Interpol) can be used as channel for communication. In order to facilitate identification of the relevant authority in another country, the United Nations Office on Drugs and Crimes (UNODC) maintains an online directory which provides the issuing authority with details of the central authority of the requested state, the channels of communication and other relevant information.[37] When submitting the request, it is necessary to meet the formal requirements as defined by paragraphs. Oral requests are only permitted in urgent cases and need to be followed by a written request. UNODC provides a software for drafting such requests with the aim of ensuring that requests are complete (Mutual Legal Assistance Request Writer Tool).[38]

Interestingly, the existing procedures for mutual legal assistance of Art. 18 UNTOC were not highlighted in the conference room paper for the second negotiating session of the Ad Hoc Committee prepared by its Chair[39] which, instead, refers to the UN Convention Against Corruption (UNCAC) in this respect and its Art. 46 UNCAC. Compared to Art. 18 UNTOC, however, there are only minor differences in paragraphs (1), (3), (9) and (24) of Art. 46 UNCAC which neither change the lack of a specific wording for data-related requests in paragraph (3)[40], nor influence the way of intelligence sharing in paragraphs (4) and (5) or the procedural aspects of mutual legal assistance in paragraphs (6)-(12)[41] or the form and content of requests as well as the channels of communication are defined in paragraphs (13)-(16) described above in the context of Art. 18 UNTOC.

[36] For details about the intention of the drafters, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, p. 225, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[37] The online directory of Competent National Authorities (CNA Directory) is available on the platform SHERLOC (SHharing Electronic Resources and Law On Crime) at: https://sherloc.unodc.org/cld/en/st/cna/CNA.html. Access requires registration and is reserved for competent national authorities. The directory indicates the central authority responsible for receiving the MLA request, languages accepted, channels of communication, contact points, fax and e-mails, specific requests of the receiving states and sometimes even extracts from domestic legislation of that state.

[38] The software is available at: https://www.unodc.org/mla/index.html.

[39] "Overview of existing instruments, recommendations and other documents on countering the use of information and communications technologies for criminal purposes", A/AC.291/CRP.10, 20 April 2022, p. 4, available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/CRP10.pdf.

[40] Art. 46(3) UNCAC merely lists the following two additional purposes for a request of mutual legal assistance:
„(j) Identifying, freezing and tracing proceeds of crime in accordance with the provisions of chapter V of this Convention" and „(k) The recovery of assets, in accordance with the provisions of chapter V of this Convention".

[41] The three subparagraphs of Art. 46(9) UNCAC address the absence of dual criminality and (a) require the requested State Party to take in to account the puposes of UNCAC, (b) grants the requested State Party the power to decline the mutual assistance requests for this reason while maintaining the obligation to render assistance that does not involve coercive action which can also be refused for specific reasons, and (c) encourages each State Party to provide a wider scope of assistance in the absence of dual criminality, nevertheless.

Therefore, the wording regarding international cooperation is essentially identical in Art. 46 UNCAC and in Art. 18 UNTOC.

The conference room paper for the second negotiating session of the Ad Hoc Committee[42] identified the following provisions as potentially useful for the elaboration of a future convention on countering the use of Information and Communication Technologies (ICTs) for criminal purposes and suggested as reference for the new convention the provisions on: the liability of legal persons (Art. 10 UNTOC), prosecution, adjudication and sanctions (Art. 11 UNTOC), international cooperation provisions such as international cooperation for the purpose of confiscation, joint investigation, training and technical assistance (Art. 29 UNTOC), the implementation of the convention (Arts. 30 and 34 UNTOC), and final provisions (Arts. 35-41 UNTOC).

2.1.3. UN Convention Against Corruption (UNCAC)

The conference room paper for the second negotiating session of the Ad Hoc Committee[43] suggested not solely Art. 46 UNCAC as reference point for regulating international cooperation in a future convention on countering the use of ICTs for criminal purposes, but UNCAC's entire Chapter IV (Art. 43-50 UNCAC) entitled "international cooperation". Therefore, it seems appropriate to point out three additional provisions in chapter IV of UNCAC:

- According to Art. 43 UNCAC, the requirement of dual criminality for international cooperation is deemed fulfilled irrespective of whether the offence is placed within the same category or denominated by the same terminology, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of the requesting as well as of the requested States Party.
- Art. 48 UNCAC, addresses the cooperation of law enforcement and requires the State Parties to enhance effectiveness of law enforcement action. This includes taking effective measures to exchange information with other States Parties concerning specific means and methods used to commit offences covered by UNCAC, including the use of false identities, forged, altered or false documents and other means of concealing activities, Art. 48(1)(d) UNCAC.
- According to Art. 50(1) UNCAC, the State Parties are obliged to allow for the appropriate use of special investigative techniques including electronic forms of surveillance and undercover operations within its territory, and to allow for the admissibility in court of evidence derived therefrom. While encouraging State Parties to enter bilateral or multilateral agreements in this respect (Art. 50(2) UNCAC), decisions are possible in the absence of such agreements and to be made on a case-by-case basis (Art. 50(3) UNCAC).

It is important to emphasise that UNCAC neither specifically concerns cybercrime nor is applicable to cybercrime. The only reason for pointing out some of its provisions is that they are suggested as reference points for the regulation of international cooperation in the conference room paper for the second negotiating

[42] "Overview of existing instruments, recommendations and other documents on countering the use of information and communications technologies for criminal purposes", A/AC.291/CRP.10, 20 April 2022, p. 4, available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/CRP10.pdf.

[43] "Overview of existing instruments, recommendations and other documents on countering the use of information and communications technologies for criminal purposes", A/AC.291/CRP.10, 20 April 2022, p. 4, available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/CRP10.pdf.

session of the Ad Hoc Committee[44]. Apart from Chapter IV of UNCAC on "international cooperation", this conference paper also suggests the following reference points as potentially useful for the elaboration of a future convention on countering the use of ICTs for criminal purposes: liability of legal persons (Art. 26 UNCAC), ancillary provisions on criminalization (Arts. 27-30 UNCAC), freezing, seizure and confiscation (art. 31), protection of witnesses, experts, victims and reporting persons (Arts. 32 -33 UNCAC), provisions related to law enforcement (Arts. 36-39 UNCAC), criminal record (Art. 41 UNCAC), jurisdiction (Art. 42 UNCAC), asset recovery (chapter V, Art. 51-59 UNCAC), technical assistance and information exchange (chapter VI, Art. 60-62 UNCAC), mechanisms for implementation (chapter VII, Art. 63-64 UNCAC), and final provisions (chapter VIII, Art. 65-71 UNCAC).

2.2. CoE Framework

In 2001, the Council of Europe (CoE) elaborated the Convention on Cybercrime which is still the only multilateral, legally binding instrument addressing criminal activity conducted via the Internet[45]. The CoE Convention on Cybercrime seeks to harmonise national laws relating to cybercrime, to improve domestic procedures for detecting, investigating, and prosecuting such crimes and to provide arrangements for fast and reliable international cooperation on these matters. The CoE Convention on Cybercrime establishes a common minimum standard for domestic computer-related offences and provides for the criminalisation of nine such offences[46], including offences relating to unauthorised access to[47] and illicit tampering[48] with computer systems, programs or data; computer-related forgery[49] and fraud[50]; and attempting, aiding or abetting the commission of such acts[51].

The CoE Convention on Cybercrime establishes mechanisms for international cooperation against cybercrime and requires States Parties to establish powers and procedures to obtain electronic evidence (section 2.2.1. below) and to provide each other mutual legal assistance (section 2.2.2. below). The electronic evidence is distinguished into *computer data, traffic data* and *subscriber information*. The term *"computer data"* refers to any representation of facts, information or concepts in a form suitable for processing in a computer system,[52] whereas *"traffic data"* means any computer data relating to a communication by means of a computer system.[53] In contrast, the term *"subscriber data"* means any information held by a service provider relating to

[44] "Overview of existing instruments, recommendations and other documents on countering the use of information and communications technologies for criminal purposes", A/AC.291/CRP.10, 20 April 2022, available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/CRP10.pdf.

[45] CoE Convention on Cybercrime, ETS No.185, Budapest, 23 November 2001 (also known as Budapest Convention) which entered into force on 1 July 2004.

[46] See Art. 2 – 10 CoE Convention on Cybercrime.

[47] Art. 2 CoE Convention on Cybercrime.

[48] Art. 5 CoE Convention on Cybercrime.

[49] Art. 7 CoE Convention on Cybercrime.

[50] Art. 8 CoE Convention on Cybercrime.

[51] Art. 11 CoE Convention on Cybercrime.

[52] Art. 1(b) CoE Convention on Cybercrime.

[53] Art. 1(d) CoE Convention on Cybercrime.

subscribers of its services other than *traffic* or *content data*.[54]

2.2.1. Collection of Digital Evidence

The procedural powers for gathering digital evidence are enshrined in Articles 14 – 21 CoE Convention on Cybercrime. According to Article 14(2) CoE Convention on Cybercrime, these procedural powers may be used in specific criminal investigations or proceedings in any type of case.

2.2.1.1. Preservation and Disclosure

Art. 16 CoE Convention on Cybercrime requests for LEAs and other competent national authorities the ability to order the expeditious preservation of specified *computer data* including *traffic data*. Such an order according to Art. 16 CoE Convention on Cybercrime obliges the Internet service provider to save the data that were processed by this provider. The provider is not forced to start collecting data it would not normally store[55] but the data which already exist have to be stored in a way that preserves its current quality and condition.[56] The provider is not obliged to transfer the relevant data to the requesting authority. Rather, Art. 16 CoE Convention on Cybercrime authorises LEAs to prevent the deletion of the relevant data.

The obligation to transfer data is regulated in Art. 17 and 18 CoE Convention on Cybercrime. By separating the obligation to preserve the data from the obligation to disclose the data the CoE Convention on Cybercrime offers the advantage of attaching different conditions to each obligation. Art. 17 CoE Convention on Cybercrime enables LEAs to order the expedited preservation and partial disclosure of *traffic data* which is extremely useful in cases requiring to trace back the route to a suspected individual and the need for immediate access to identify the path through which this communication was transmitted. Based on Art. 18 CoE Convention on Cybercrime, a provider can be obliged to disclose the data which it has preserved. The preservation of the data does not have to be based on a previous preservation order[57]. Rather, Art. 18(a) CoE Convention on Cybercrime provides a general instrument for LEAs which is especially useful in cases not requiring access to hardware.[58] Article 18(b) CoE Convention on Cybercrime enables LEAs to order the submission of subscriber information which is an extremely useful tool in cases requiring IP-based investigations. If a cybercrime investigator has identified an IP-address which was used in connection with an offence, then there is a need to identify the person who used this IP-address at the time of the offence. Based on Art. 18(1)(b) CoE Convention on Cybercrime the provider is obliged to submit the subscriber information defined in Art. 18(3) CoE Convention on Cybercrime.

[54] Art. 18(3) CoE Convention on Cybercrime.

[55] See No. 152 of the Explanatory Report to the CoE Convention on Cybercrime.

[56] See No. 159 of the Explanatory Report to the CoE Convention on Cybercrime.

[57] Based on Article 16 CoE Convention on Cybercrime.

[58] Gercke, "Understanding Cybercrime: phenomena, challenges and legal response", ITU 2012, at 6.5.3, p. 248.

2.2.1.2. Search and Seizure

Art. 19 CoE Convention on Cybercrime introduces a data-related search and seizure procedure but does not specify the requirements which have to be met by investigators to carry out such investigations. Art. 19 (1) CoE Convention on Cybercrime aims to establish an instrument that enables the search of computer systems which is as efficient as traditional procedures.[59] If the investigator of a LEA discovers during such a search that relevant information is stored on another computer system (e.g. cloud computing), Art. 19 (2) CoE Convention on Cybercrime addresses the need to extend the search to that other system. Art. 19 (3) CoE Convention on Cybercrime provides 4 important measures for receiving evidence which is acceptable in court proceedings: (a) an instrument to seizure a computer system, (b) an instrument to copy the data, (c) to maintain the integrity of copied data[60], and (d) an instrument that allows them to remove the data if it is illegal content or to ensure at least that this illegal content data can no longer be accessed.

Last but not least, Art. 19 (4) CoE Convention on Cybercrime enables the investigator of a LEA to compel a system administrator to assist LEAs because it is necessary for LEAs to identify the exact location of suspicious data. This provision not only obliges the system administrator to provide the necessary information to the investigator, but also relieves the system administrator from contractual obligations or orders by his supervisors.[61] The scope of the obligation to support the investigator of a LEA extends only as far "as is reasonable", but the CoE Convention on Cybercrime does not define the term "reasonable". According to the Explanatory Report "reasonable" may include disclosing a password or other security measure, but does not in general cover such disclosure where this would go along with unreasonable threats to the privacy of other users or data not included in the current search.[62]

2.2.1.3. Types of Data

Under the CoE Convention on Cybercrime, the term "*traffic data*" refers to data generated by computers during the communication process in order to route a communication from its origin to its destination. Therefore, "*traffic data*" includes IP-addresses identifying the partners of an Internet-related communication.[63] Art. 20 CoE Convention on Cybercrime introduces two different ways to collect *traffic data*: The *first* way of collecting such *traffic data* is according to Art. 20(1)(a) CoE Convention on Cybercrime to impose an obligation on an Internet service provider to enable LEAs to collect the relevant data directly which generally requires the installation of an interface for LEAs to access the provider's infrastructure.[64] The *second* way enables LEAs to compel an Internet service provider according to Art. 20(1)(b) CoE Convention on Cybercrime to collect data at their request allowing LEAs to benefit from the technical capacities and the knowledge of the provider.

One of the major difficulties for investigations based on Art. 20 CoE Convention on Cybercrime is the use of

[59] This instrument has to be supplemented, see No. 187 of the Explanatory Report to the CoE Convention on Cybercrime.

[60] See No. 197 of the Explanatory Report to the CoE Convention on Cybercrime.

[61] See No. 201 of the Explanatory Report to the CoE Convention on Cybercrime.

[62] See No. 202 of the Explanatory Report to the CoE Convention on Cybercrime.

[63] See No. 30 of the Explanatory Report to the CoE Convention on Cybercrime.

[64] See No. 220 of the Explanatory Report to the CoE Convention on Cybercrime.

means of anonymous communication. Similarly, the use of public internet terminals creates a comparable anonymity for its users, although the Court of Justice of the European Union has introduced a duty to identify users of a public WLAN to avoid liability for copyright and other offences committed using this WLAN.[65]

Art. 21 CoE Convention on Cybercrime provides the possibility for LEAs to record data communications and to analyse the content if the LEAs already know who the communication partners are but have no information about the type of information exchanged. The *content data* affected by this provision includes files downloaded from websites or file-sharing systems, e-mails and chat/VoIP conversations. One of the most important difficulties for investigations based on Article 21 CoE Convention on Cybercrime is the use of encryption technology.[66]

2.2.2. Mutual Legal Assistance

The CoE Convention on Cybercrime addresses the increasing importance of international cooperation in its Art. 23 to 35. Art. 23 CoE Convention on Cybercrime defines the extent, scope and priority of international cooperation in cybercrime investigations among Parties to the CoE Convention on Cybercrime in three general principles: (1) Parties are supposed to provide each other cooperation in international investigations to the widest extent possible; (2) the general principles are applicable in any investigation involving the need to collect evidence in electronic form; and (3) the provisions of the CoE Convention on Cybercrime substitute neither provisions of international agreements pertaining to mutual legal assistance and extradition nor relevant provisions of domestic law pertaining to international cooperation.

The drafters of the CoE Convention on Cybercrime emphasized that mutual legal assistance (MLA) should in general be carried out through the application of relevant treaties and similar arrangements for MLA. As a consequence, the CoE Convention on Cybercrime does not intend to create a separate general regime on MLA.[67]

The CoE Convention on Cybercrime requires Parties to adopt a set of procedural powers to secure electronic evidence, such as search and seizure of computer systems[68], production orders for data[69], interception of communications[70]. These are subject to rule of law safeguards. They apply to electronic evidence in relation to any crime.

In the course of cybercrime investigations, a core difficulty for national LEAs is that electronic evidence needed is increasingly available only in foreign, sometimes unknown, multiple or shifting jurisdictions. MLA arrangements appear not always feasible or too cumbersome to secure volatile electronic evidence, although Art. 25 CoE Convention on Cybercrime highlights the importance of fast communication and Art. 26 CoE

[65] CJEU, decision of 15 September 2016 in case C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*; Bisle/Frommer, CR 2017, pp. 54-63.

[66] Gercke, "Understanding Cybercrime: phenomena, challenges and legal response", ITU 2012, at 6.5.3, p. 259.

[67] Gercke, "Understanding Cybercrime: phenomena, challenges and legal response", ITU 2012, at 6.6.5, p. 274.

[68] Art. 19 CoE Convention on Cybercrime.

[69] Art. 16, 17 and 18 CoE Convention on Cybercrime.

[70] Art. 21 CoE Convention on Cybercrime.

Convention on Cybercrime sets out regulations necessary for LEAs to inform foreign LEAs without jeopardising their own investigation. This is hardly surprising because both formal processes were developed to protect the integrity of a Party as a state as well as to safeguard the rights of the accused.[71] Bearing in mind the principle of national sovereignty, the procedural instruments provided by the CoE Convention on Cybercrime can only be used for investigations at the national level. If cybercrime investigators realise that evidence has to be collected outside their national territory, they need to request MLA.

Except for one, all procedural instruments for gather digital evidence established in the Art. 16 – 21 CoE Convention on Cybercrime[72] have a corresponding provision in the Art. 28 – 33 CoE Convention on Cybercrime enabling LEAs to apply the procedural instruments upon request of a LEA in another jurisdiction. Only Art. 18 CoE Convention on Cybercrime on production orders including on subscriber information has no corresponding provision in Chapter III on international co-operation of the CoE Convention on Cybercrime. However, the Cybercrime Convention Committee (T-CY) adopted a Guidance Note on the Production of Subscriber Information (Article 18 CoE Convention on Cybercrime) in 2017.[73] This Guidance Note provides criminal justice authorities with the ability to request a service provider offering its service in the territory of a Party to produce subscriber information for example of a webmail or a social media account even if the data or the provider are in another Party's jurisdiction. Consequently, Art. 18 CoE Convention on Cybercrime could serve as the domestic legal basis.

2.2.3. Publicly Available Data and Individual Consent

The CoE Convention on Cybercrime provides in its Art. 32 two scenarios in which a Party may have access to stored *computer data* without the authorisation of another Party: The *first scenario* concerns access to publicly available (open source) stored *computer data* regardless of where the data is located geographically[74]. An example of such publicly available data is information made available on websites without access control (such as passwords). If cybercrime investigators were not allowed to access these websites, this could seriously hamper their investigation. The *second scenario* concerns access to data based on the consent of the person in control of this data[75]. When an investigator has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data, the investigator may access this data.

Whereas the first scenario appears widely accepted, the second scenario raises serious concerns because it probably contradicts fundamental principles of international law. Based on international law, investigators have to respect national sovereignty during an investigation.[76] Investigators are especially not allowed to carry

[71] Gercke, "Understanding Cybercrime: phenomena, challenges and legal response", ITU 2012, at 6.6.5, p. 276.

[72] Chapter III. on International co-operation of the CoE Convention on Cybercrime.

[73] Cybercrime Convention Committee (T-CY), "T-CY Guidance Note #10 on Production Orders for Subscriber Information (Art. 18. Budapest Convention)", adopted on 1 March 2017, available at: https://ccdcoe.org/uploads/2018/11/COE-170228-GN10-1.pdf.

[74] Art. 32(a) CoE Convention on Cybercrime.

[75] Art. 32(b) CoE Convention on Cybercrime.

[76] National sovereignty is a fundamental principle in international law, see: Roth, "State Sovereignty, International Legality, and Moral disagreement, 2005, p. 1, available at:

out investigations in another state without the consent of the competent authorities in that state. The decision whether such permission should be granted is not in the hands of an individual, but of the state authorities because interference with national sovereignty not only affects the rights of the individual, but also state concerns. However, it may be argued that Parties ratifying the CoE Convention on Cybercrime partly waive their protection by the principle of national sovereignty and allow other countries to carry out investigations affecting their territory.[77] This argument is supported by the Guidance Note of the Cybercrime Convention Committee on the interpretation of Article 32(b) CoE Convention on Cybercrime which points out that this provision would not cover situations where the data are not stored in another Party or where it is uncertain where the data are located.[78]

Other concerns regarding the second scenario are that Art. 32(b) CoE Convention on Cybercrime neither defines any procedures for the investigation nor safeguards the suspect's right to privacy, right to protection of his personal data and procedural rights. The wording of this provision seems to suggest that not even limitations of national law are applicable which would apply to identical domestic investigations. However, the Guidance Note of the Cybercrime Convention Committee on the applicable law points out that access to data would not be permitted under Art. 32(b) CoE Convention on Cybercrime if access or disclosure was not permitted domestically.[79] Further, it has to be pointed out that LEAs may only seek (!) permission of the person who has the lawful authority to disclose the data. This contrasts starkly with the instrument of a production order according to Art. 18 CoE Convention on Cybercrime. Finally, it has to be pointed out that the standard hypothesis underlying Art. 32(b) CoE Convention on Cybercrime is that the person contacted to provide access to the data is physically located in the territory of the requesting Party leading the Cybercrime Convention Committee to suggest in its Guiding Note that LEAs should take into account that many Parties would object or consider it a criminal offence, if a person who is physically in their territory is directly approached by foreign LEAs seeking his or her cooperation.[80]

2.2.4. The 24/7 Network of Contacts

To increase the speed of international investigations, the CoE Convention on Cybercrime not only highlights in its Art. 25 the importance of enabling the use of expedited means of communication, but also obliges its Parties in its Art. 35 to designate a contact point for MLA requests which is available without any time limitations. To improve the efficiency of MLA requests, the Parties are obliged to establish these contact points

https://www.yumpu.com/en/document/view/4246351/state-sovereignty-international-legality-and-moral-disagreement-.

[77] Gercke, "Understanding Cybercrime: phenomena, challenges and legal response", ITU 2012, at 6.6.5, pp. 277-278.

[78] Cybercrime Convention Committee, T-CY Guidance Note on Transborder Access to Data (Article 32), adopted on 2-3 December 2014, T-CY(2013)29rev, 8 December 2014, p. 22 on the notion of "transborder" and "location".

[79] T-CY Guidance Notes, T-CY(2013)29rev, 8 December 2014, p. 22 on the applicable law regarding Transborder Access to data (Article 32).

[80] T-CY Guidance Notes, T-CY(2013)29rev, 8 December 2014, p. 23 on the location of the person consenting to provide access or disclose data regarding Transborder Access to data (Article 32).

and to ensure that they are able to carry out certain immediate action[81] as well as to maintain their service[82].

The CoE Convention on Cybercrime does not prescribe which national authority should be responsible for operating the national contact point of the 24/7 network. Nevertheless, the idea of the 24/7 network of contact points provides a useful answer to the challenges of fighting cybercrime associated especially with the speed of data exchange processes. Unfortunately, a study carried out in 2009 on the functioning of 24/7 points of contact in an international network fighting cybercrime[83] revealed that the full potential of such a network is not (yet) used because not all Parties of the CoE Convention on Cybercrime had created a functioning contact point and not all contact points were used to their full capacity or known domestically.

2.2.5. Second Additional Protocol to CoE Convention on Cybercrime

With the aim of moving away from data storage location as a decisive factor, the CoE Committee of Ministers adopted a Second Additional Protocol[84] to the CoE Convention on Cybercrime on 17 November 2021. This Second Additional Protocol addresses the challenges to criminal justice in cyberspace and provides for enhanced and more effective cooperation and disclosure of electronic evidence. More specifically, the Second Additional Protocol aims to further enhance co-operation on cybercrime and the ability of criminal justice authorities to collect evidence in electronic form of a criminal offence for the purpose of specific criminal investigations or proceedings through:

- additional tools pertaining to more efficient mutual assistance and other forms of co-operation between competent authorities;
- co-operation in emergencies (that is, in situations where there is a significant and imminent risk to the life or safety of any natural person); and
- direct co-operation between competent authorities and service providers and other entities in possession or control of pertinent information.[85]

The Second Additional Protocol was opened for signature and signed by 22 State Parties[86] in May 2022 after

[81] Article 35(1) CoE Convention on Cybercrime mentions as measures (a) technical advice, (b) preservation of data and (c) the collection of evidence, the provision of legal information and locating of suspects.

[82] Article 35(2) CoE Convention on Cybercrime requires for such a contact point (a) the capacity to carry out communications on an expedited basis and (b) the ability to co-ordinate with other national authorities on an expedited basis.

[83] CoE Economic Crime Division, „The functioning of 24/7 points of contact for cybercrime“, Discussion Paper, 2 April 2009.

[84] CoE, Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Draft Protocol version 2, 12 April 2021.

[85] CoE, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Special Edition of 17 November 2021, Explanatory Report, para. 26, p. 38, available at: https://rm.coe.int/special-edition-second-protocol-en-2021/1680a69930.

[86] The following 22 State Parties signed the Second Additional Protocol on 12 May 2022: Austria, Belgium, Bulgaria, Chile, Colombia, Estonia, Finland, Iceland, Italy, Japan, Lithuania, Luxembourg, Montenegro, Morocco, Netherlands, North Macedonia, Portugal, Romania, Serbia, Spain, Sweden and the United States of America.

which 14 more State Parties[87] have signed. Pursuant to Art. 16(3) Second Additional Protocol, five State Parties have to ratify the Second Additional Protocol for it to enter into force in the month following the last ratification. So far, Serbia is the only State Party having ratified the Second Additional Protocol in February 2023.[88]

While Art. 3(1) Second Additional Protocol incorporates the definitions provided in the CoE Convention on Cybercrime for *"computer data"*, *"traffic data"* and *"subscriber information"*, the methods of co-operation are contained in Chapter II Second Additional Protocol and each type of co-operation is governed by different principles. For this reason, this Chapter II is divided into the following five sections:[89] (1) general principles, Art. 5 Second Additional Protocol; (2) procedures enhancing direct co-operation with providers and entities in other State Parties, Art. 6-7 Second Additional Protocol; (3) procedures enhancing international co-operation between authorities for the disclosure of stored *computer data*, Art. 8-9 Second Additional Protocol; (4) procedures pertaining to emergency mutual assistance, Art. 10 Second Additional Protocol; and (5) procedures pertaining to international co-operation in the absence of applicable international agreements, Art. 11-12 Second Additional Protocol.

Art. 6 and 7 Second Additional Protocol permit the competent authority of one State Party to engage directly with private entities possessing or controlling the sought information and located in the territory of a second State Party, whether a MLAT between the two interested State Parties exists or not. Whereas Art. 6 Second Additional Protocol relates to information "*for identifying or contacting the registrant of a domain name*", Art. 7 Second Additional Protocol relates to "*subscriber information*".

Art. 8 Second Additional Protocol provides for State Parties to adopt any legislative measure as necessary to issue orders incoming from another State Party and addressing OSPs located in its territory for the production of *subscriber information* and *traffic data*. The strict deadlines introduced for the OSP's response ensure significantly expedited production of the data (20 days for *subscriber information* and 45 days for *traffic data*).

Art. 9 Second Additional Protocol requires that the 24/7 Network of Contacts to be able to transmit and receive requests from a Point of Contact in another State Party seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored *computer data* in that service provider's possession or control, and without the need for a request for mutual legal assistance.

2.3. EU Framework

This section describes first the existing mechanisms for international cooperation under Directive (EU) 2014/41 (section 2.3.1. below) and then the new mechanisms according to the proposed eEvidence Package (section 2.3.2. below) as well as the proposed Police Cooperation Code (section 2.3.3. below).

[87] These 14 further signatories are: Andorra on 20 May 2022; Costa Rica on 13 June 2022; Croatia, Moldovia, Slovenia, Sri Lanka, Ukraine and the United Kingdom on 30 November 2022; Greece on 20 January 2023; France and Germany on 27 January 2023; Dominican Republic on 30 January 2023; Argentina on 16 February 2023; Albania on 27 February 2023.

[88] According to the chart of signatures and ratifications of Treaty CETS No. 224, Serbia ratified the Second Additional Protocol on 9 February 2023: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 (last accessed on 26 March 2023).

[89] CoE, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Special Edition of 17 November 2021, Explanatory Report, para. 29, p. 39, available at: https://rm.coe.int/special-edition-second-protocol-en-2021/1680a69930.

2.3.1. Directive (EU) 2014/41

The main legal instrument at disposal of EU MS seeking electronic data of OSPs established in other EU MS within the framework of criminal proceedings is the *European Investigation Order* (EIO) established by Directive (EU) 2014/41.[90] The EIO is a judicial decision, issued or validated by a judicial authority of one Member State (the "*issuing Member State*"), to have one or several specific investigative measure(s) carried out in another Member State (the "*executing Member State*") to obtain evidence. Applicable investigative measures include, among others, interception of telecommunications and preservation of (electronic) evidence. The only types of evidence gathering that are excluded from Directive (EU) 2014/41 are the establishment of a Joint Investigation Team, and the collection of evidence within its framework; and cross-border surveillance provided for in the Convention Implementing the Schengen Agreement[91].

From a cybercrime investigator's point of view, Directive (EU) 2014/41 not only approximates the handling of international cooperation cases to the handling of domestic cases,[92] but also introduced the possibility of cross-border real-time gathering of evidence allowing access to and transfer of both, telecommunications *traffic* and *location data* as well as *content data*. However, Directive (EU) 2014/41 does not contain specific provisions related to accessing electronic data, except for Art. 10(2)(e) Directive (EU) 2014/41, which concerns the identification of a person holding an IP address.

Further, the timeframe of 30 plus 90 days, while representing a step forward compared to previously existing instruments, is still insufficient to properly address the volatile and dynamic field of electronic data. Especially since this deadline may be extended in certain cases (e.g. if the execution of the EIO has the potential to prejudice an ongoing criminal investigation or prosecution, or if the objects, documents, or data concerned are already being used in other proceedings)[93].

Another limit of Directive (EU) 2014/41 is that Ireland and Denmark are neither bound by it nor subject to its application, based on Articles 1 and 2 of Protocol No 21 and Articles 1 and 2 of Protocol No 22 annexed to the Treaty of the European Union (TEU). Because several OSPs receiving high numbers of requests are based in Ireland (like Airbnb, Apple, Facebook, Google, Microsoft, Twitter, Verizon Media),[94] the scope of Directive (EU) 2014/41 seems significantly limited.

---

[90] Directive (EU) 2014/41 is transposed in all EU Member States since 2017.

[91] Convention Implementing the Schengen Agreement of 14 June 1985 between Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on gradual abolition of the checks at their common borders, 22 September 2000, Official Journal of the European Communities L 239, p. 19. In this context, see also Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), 23 March 2016 Official Journal of the EU, L 77, p. 1.

[92] An EIO is to be treated and executed like comparable domestic cases and comes with precise deadlines: 30 days for the decision on the recognition of the order, and 90 days for the execution of the order, Art. 12 (3) and (4) Directive (EU) 2014/41. It should be noted that the existence of a similar offence in the national legislation of the two or more Member States involved (*double criminality*) is not required by Directive (EU) 2014/41 for an EIO, but is an optional ground for refusal of an EIO.

[93] Article 15 of Directive 2014/41/EU.

[94] Europol, Eurojust, EJN, 2020.

2.3.2. Draft eEvidence Package

In April 2018, the European Commission presented a legislative package on electronic evidence consisting of a proposal for a Regulation on European Production and Preservation Orders in criminal matters (Draft eEvidence Regulation)[95] and a proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (Draft eEvidence Directive).[96] The Draft eEvidence Package entered the trilogue stage of the legislative process in February 2021[97] and the final compromise text for both, the eEvidence Directive as well as for the eEvidence Regulation was agreed upon almost two years later in January 2023.[98] The eEvidence Regulation[99] aims to introduce binding European Production and Preservation Orders which can be issued to seek preservation or production of data that are stored by a service provider located in another jurisdiction and that are necessary as evidence in criminal investigations or criminal proceedings.[100]

The categories of data that can be obtained with a European Production Order by the competent authorities include *"subscriber data", "data requested for the sole purpose of identifying the user"* and *"traffic data"* (the three categories commonly referred to jointly as '*non-content data*') and stored *content data*. This distinction exists in the legal orders of many Member States and also in non-EU legal frameworks.[101] According to Art. 2(6) eEvidence Regulation, '*electronic evidence*' means *subscriber data*, *traffic data* or *content data* stored by or on behalf of a service provider, in an electronic form, at the time of receipt of a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR).[102] The term *"subscriber data"* means any data held by a service provider relating to the subscription to the services, pertaining to the identity of a subscriber and to the type of service and its duration.[103] The term "*traffic data*" refers to data related to

[95] Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17 April 2018.
[96] Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, 17 April 2018.
[97] See Council of the EU, "E-Evidence Package: First Trilogue Meeting", 10 February 2021, available at: https://www.2021portugal.eu/en/news/e-evidence-package-first-trilogue-meeting/.
[98] Council of the EU, „Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence", Press Release 48/23, 25 January 2023, available at: https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/.
[99] Council of the EU, Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, final compromise text, 5448/23, 20 January 2023, available at: https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf.
[100] Commission, Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17 April 2018, p. 4.
[101] Commission, Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17 April 2018, p. 14.
[102] The definition of ‚electronic evidence' in Art. 2(6) of the Commission's Draft e-Evidence Regulation had referred to „ evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a Production or Preservation Order certificate, consisting in stored *subscriber data*, *access data*, *transactional data* and *content data*".
[103] Art. 2(7) eEvidence Regulation.

the provision of a service offered by a service provider that serves to provide context or additional information about such service and includes metadata.[104] The term *"content data"* means any data in a digital format such as text, voice, videos, images, and sound.[105] In addition, the term *"data requested for the sole purpose of identifying the user"* refers IP addresses as well as the relevant source ports and time stamp (date/time), or technical equivalents of these identifiers and related information where requested by LEAs for the sole purpose of identifying the user in a specific criminal investigation.[106]

In the context of cybercrime investigations, it is important to point out that the final compromise text of the eEvidence Directive[107] envisions to introduce an obligation for OSPs to appoint a legal representative in the EU Member State where it is established or with which the OSP has a "substantial connection".[108] According to Recital 13 eEvidence Directive a "substantial connection" means that (a) the OSP enables legal or natural persons in the EU to use its services, and (b) is established in the EU or (c) there is a significant number of users of its services in one or more EU MS, or (d) it targets its activities towards one or more EU MS (for example based on the language it uses to promote its services, or on the currency allowed for transactions). Bearing in mind that neither Denmark nor Ireland participate in the judicial cooperation instruments adopted under Title V, Chapter 4, of the TFEU, leaving the choice of the EU Member State for legal representative to the OSP seems to risk effectiveness. However, the legal representative should be empowered by the OSP to respond to and execute the Preservation and Production Orders introduced by the eEvidence Regulation.

The eEvidence Regulation envisions to introduce two new legal instruments for access to electronic evidence:

- The **European Production Order** aims at gaining access to *electronic evidence* (= *subscriber data*, *traffic data* or *content data*).[109]
- The **European Preservation Order** aims at preserving *electronic evidence* by freezing a set of data to avoid its loss.[110]

Both orders are served by competent authorities of an EU Member State[111] (depending on the category of data sought, different authorities may have competence) either to the *designated establishment*[112] or to the *legal representatives*[113] designated by the relevant OSP.[114]

Together, the eEvidence Regulation and the eEvidence Directive (eEvidence Package) offer several improvements for future cybercrime investigations. *First*, by moving away from considering data location as a

[104] Art. 2(9) eEvidence Regulation. The Commission had proposed to term this kind of data "transactional data", Art. 2(9) Draft eEvidence Regulation.
[105] Art. 2(10) eEvidence Regulation.
[106] Art. 2(8) eEvidence Regulation. The term *"data requested for the sole purpose of identifying the user"* has evolved in the course of the legislative process. The Commission had originally proposed in Art. 2(8) Draft eEvidence Regulation to define a term *"access data"* as referring to data related to the commencement and termination of a user access session to a service.
[107] Council of the EU, Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, final compromise text, 5449/23, 20 January 2023, available at: https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/en/pdf.
[108] Art. 3(1) in conjunction with Art. 2(3) eEvidence Directive.
[109] Art. 2(1) eEvidence Regulation.
[110] Art. 2(2) eEvidence Regulation.
[111] Art. 4 eEvidence Regulation.
[112] Defined in Art. 2(5a) eEvidence Regulation.
[113] Defined in Art. 2(5b) eEvidence Regulation.
[114] Art. 7(1) eEvidence Regulation.

determining connecting factor and preferring the economic presence, the eEvidence Package has the potential to overcome key challenges encountered currently in establishing jurisdiction, and proves to be fit for modern technologies such as the cloud, which transcend traditional territorial borders. *Second*, the eEvidence Package creates a direct link with the OSP, thus avoiding the additional step of traditional MLA procedures where the judicial authority of the foreign country needs to be involved. This potentially shortens the overall timeframe, as well as the administrative burden. *Third*, the eEvidence Package creates a mandatory framework, introducing short deadlines[115], enforcement mechanisms[116] and sanctions[117] for non-compliance. *Finally*, the eEvidence package includes five clear and user-friendly forms in its annexes,[118] thus standardising the channels for cooperation.

Because the legislative processes of the eEvidence Regulation as well as of the eEvidence Directive are pending until their final versions have been published in the Official Journal of the EU, the current EU legal framework consists of Union cooperation instruments in criminal matters, such as the Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO Directive)[119] and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[120] Referring to national Member State law, the EIO Directive itself neither defines the term evidence nor distinguishes different types of data.

2.3.3. Draft Police Cooperation Code

Most relevant for the development of the GRACE solution and the international cooperation between LEAs in EU Member States, the European Commission presented a proposal for an EU Police Cooperation Code in December 2021. The EU Police Cooperation Code aims not only to enhance law enforcement cooperation across Member States but also to give EU police officers more modern tools for information exchange. For that purpose, the proposed EU Police Cooperation Code comprises three elements: (i) a Regulation on Automated Data Exchange for Police Cooperation ("Prüm II")[121]; (ii) a Directive on Information Exchange

[115] 10 days, pursuant Art. 9(1) eEvidence Regulation, which become 8 hours in cases of emergency or 96 hours after a mandatory prior notification Art. 9(2) eEvidence Regulation.
[116] Art 14 eEvidence Regulation. In comparison, the EU-US MLAT will only include enforceable mechanisms when the executive agreement under the Cloud Act is signed. The CoE Convention on Cybercrime will become mandatory only once its Second Additional Protocol is signed by all Parties.
[117] Art. 13 eEvidence Regulation.
[118] The five forms are: the "European Production Order Certificate (EPOC) for the production of electronic evidence" in Annex I; the "European Preservation Order Certificate (EPOC-PR) for the preservation of electronic evidence" in Annex II, the "Information on the impossibility to execute the EPOC / EPOC-PR" in Annex III, the "Confirmation of Issuance of request for production following a European Preservation Order" in Annex IV and the "Extension of the preservation of electronic evidence" in Annex V of the eEvidence Regulation.
[119] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, 1 May 2014, Official Journal of the EU L 130, p.1.
[120] Council Act of 29 May 2000 establishing in accordance with Article 34 TEU the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU, 12 July 2000, Official Journal of the EC, 43 C 197, p. 1.
[121] Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council,

between MS LEAs[122]; and (Iii) a Council Recommendation on Operational Police Cooperation[123].

The Draft Prüm II Regulation is *lex specialis* to the Draft Directive on Information Exchange between MS LEAs and aims to facilitate automated data exchange between LEAs in different Member States and with Europol as the EU criminal information hub.[124] By introducing facial images, police records and driving licence data as additional categories data eligible to automated comparison, the Draft Prüm II Regulation proposes the introduction of a new infrastructure for standardised procedures identifying a match of core data.

As technological architecture for such queries, the Draft Prüm II Regulation envisages the creation of two central routers (the Prüm II router[125] for comparisons of biometric data and the European Police Records Index System[126] for comparisons of police records), each acting as a connecting infrastructure point between Member States. This hybrid approach between a decentralised and centralised solution avoids any data storage at central level by connecting national databases in each Member State to the central router instead of connecting to one another and establishing each router as message broker forwarding search transactions and replies to national systems, without creating new data processes, enlarging access rights or replacing national databases.[127] The Router is to be developed and managed by European Union Agency for the Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice (eu-LISA).[128]

While the Draft Prüm II Regulation has already foreseen to confer implementing powers to the European Commission, in general, regarding the technical arrangements and specifications for automated searching procedures, the standards for data exchange and the data elements to be exchanged,[129] the General Approach of the Council includes an additional Art. 23a on principles for the exchange of facial images, in particular, introducing a key role of the European Commission in specifying (1) the relevant European or international standards for facial images exchange to be used by Member States and Europol, and (2) a minimum quality

---

COM/2021/784 final, 8 December 2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:784:FIN.

[122] Proposal for a Regulation of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM/2021/782 final, 8 December 2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:782:FIN.

[123] Proposal for a Council Recommendation on operational police cooperation, COM/2021/780 final, 8 December 2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:780:FIN.

[124] Proposal for a Regulation of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM/2021/782 final, 8 December 2021, Explanatory Memorandum, p. 2.

[125] Art. 35 Draft Prüm II Regulation.

[126] Defined as EPRIS in Art. 42 Draft Prüm II Regulation.

[127] Art. 37 Draft Prüm II Regulation for the ‚Prüm II router' and Art. 44 Draft Prüm II Regulation for EPRIS. See also: Proposal for a Regulation of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM/2021/782 final, 8 December 2021, Explanatory Memorandum, p. 4.

[128] Recital 23 Draft Prüm II Regulation highlighting the necessity, for this purpose to amend Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (OJ L 295, 21.11.2018, p. 99).

[129] Recital 21 Draft Prüm II Regulation.

standard for the comparison of facial images.[130] The EU-Parliament has not yet adopted its position, but the LIBE Committee's Draft Report seems to agree with the need for inserting an additional Art. 23a on principles for the exchange of facial images granting a key role of the Commission as expressed in the Council's General Approach.[131]

Europol is envisioned to form an integral part of the framework established by the Draft Prüm II Regulation by making biometric data obtained through third countries available to MS LEAs for automated comparisons, on the one side, and by enabling Europol to automatically check its third country-sourced data against Member States' national databases.[132] Under the framework of the Draft Prüm II Regulation, simultaneous queries with biometric data will be permitted in national databases of Member States as well as in the Europol database.[133]

According to Art. 23(1) Draft Prüm II Regulation, a comparison of facial images is initiated by a request for an automated search which includes the facial images to be compared and their national reference number[134]. The answer to such a request then includes not only the matching facial images,[135] but also their national reference number[136] and code[137] in the requested Member State, Art. 23(2) Draft Prüm II Regulation. While the European Commission's proposal includes the obligation for Member States to allow national contact points of other Member States and Europol access to the "facial images" stored in their national databases[138], the General Approach of the Council suggests to allow such access only to the "facial images reference data" so that an automated search can be conducted solely by "comparing facial images reference data"[139] and the

[130] Council of the EU, „Council adopts two general approaches and a recommendation to improve operational police cooperation and information exchange", Press Release, 10 June 2022, linking to the General Approach of the Council on the Draft Prüm II Regulation, No. 9544/22, 31 May 2022, available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/10/council-adopts-recommendation-two-negotiating-mandates-improve-operational-police-cooperation-information-exchange/. See also Art. 22(3) Draft Prüm II Regulation regarding a minimum standard for facial recognition.
[131] EU-Parliament, LIBE Committee, Draft Report on Draft Prüm II Regulation, 2021/0410(COD), 19 September 2022, Amendment 103, p. 53; available at: https://www.europarl.europa.eu/doceo/document/LIBE-PR-736469_EN.pdf.
[132] Proposal for a Regulation of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM/2021/782 final, 8 December 2021, Explanatory Memorandum, p. 4.
[133] Art. 37(1) Draft Prüm II Regulation for simultaneous searches in all or selected databases of Member States or Europol regarding facial images and Art. 42(2)(a) Draft Prüm II Regulation regarding police reports.
[134] According to Art. 23 Draft Prüm II Regulation, the national „reference number" is a combination of (a) a reference number allowing Member States, in case of a match, to retrieve further data and other information in their databases for sharing, and (b) a code to indicate the Member State which holds the facial images.
[135] Art. 24(2)(f) Draft Prüm II Regulation.
[136] Art. 24(2)(e) Draft Prüm II Regulation.
[137] Art. 24(2)(d) Draft Prüm II Regulation.
[138] Art. 22(1) Draft Prüm II Regulation.
[139] Art. 22(1) in the General Approach of the Council on the Draft Prüm II Regulation, No. 9544/22, 31 May 2022, adopted on 10 June 2022, available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/10/council-adopts-recommendation-two-negotiating-mandates-improve-operational-police-cooperation-information-exchange/

Parliament's Draft Report appears to agree with limiting access to only "facial images reference data"[140].

This delta in the potential wording for a future Prüm II Regulation mirrors the delta regarding the scope of Member State's obligation to include facial images in their national databases: While the European Commission's proposal included the obligation for Member States to ensure the availability of facial images from their national databases established for the prevention, detection and investigation of criminal offences[141] and Parliament's Draft Report seems to agree with this requirement merely limiting it to facial images of suspects and convicted persons[142], the General Approach of the Council suggests to reduce this obligation to ensuring such availability only for the "facial images reference data"[143].

Any matches resulting from a query in requested Member States' databases and Europol data shall be sent back in an automated manner to the router[144] which then ranks the replies in accordance with the score of the correspondence between the biometric data used for querying and the biometric data stored in the Member States' databases and Europol data[145]. The list of matching facial images and their scores are automatically returned by the router[146] and the result of a successful automatic search is to be followed by the exchange of core data within a tight deadline[147]. Whereas the European Commission's proposal set a deadline of "within 24 hours"[148], the General Approach of the Council suggested to extend this deadline to "within 72 hours" and to enumerate in detail the conditions and the path ("via the router") of such exchange of core data[149]. In contrast, Parliament's Draft Report appears to agree with the shorter deadline of 24 hours as default, but suggests to extend this deadline to 72 hours where a judicial authorisation is required under national law.[150]

It is very interesting to note that Art. 48 Draft Prüm II Regulation establishes the platform Secure Information

---

[140] EU-Parliament, LIBE Committee, Draft Report on Draft Prüm II Regulation, 2021/0410(COD), 19 September 2022, Amendment 98, p. 51; available at: https://www.europarl.europa.eu/doceo/document/LIBE-PR-736469_EN.pdf.
[141] Art. 21(1) Draft Prüm II Regulation.
[142] EU-Parliament, LIBE Committee, Draft Report on Draft Prüm II Regulation, 2021/0410(COD), 19 September 2022, Amendment 95, p. 49; available at: https://www.europarl.europa.eu/doceo/document/LIBE-PR-736469_EN.pdf.
[143] Art. 21(1) in the General Approach of the Council on the Draft Prüm II Regulation, No. 9544/22, 31 May 2022, adopted on 10 June 2022, available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/10/council-adopts-recommendation-two-negotiating-mandates-improve-operational-police-cooperation-information-exchange/
[144] Art. 37(3) Draft Prüm II Regulation. Parliament's Draft Report suggests to add that requesting Member State shall be notified in an automated manner where there is no match: EU-Parliament, LIBE Committee, Draft Report on Draft Prüm II Regulation, 2021/0410(COD), 19 September 2022, Amendment 131, p. 64; available at: https://www.europarl.europa.eu/doceo/document/LIBE-PR-736469_EN.pdf.
[145] Art. 37(4) Draft Prüm II Regulation.
[146] Art. 37(5) Draft Prüm II Regulation.
[147] Art. 47 Draft Prüm II Regulation.
[148] Art. 47(1) Draft Prüm II Regulation.
[149] Art. 47(1) in the General Approach of the Council on the Draft Prüm II Regulation, No. 9544/22, 31 May 2022, adopted on 10 June 2022, available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/10/council-adopts-recommendation-two-negotiating-mandates-improve-operational-police-cooperation-information-exchange/
[150] EU-Parliament, LIBE Committee, Draft Report on Draft Prüm II Regulation, 2021/0410(COD), 19 September 2022, Amendment 156, p. 73 et seq.; available at: https://www.europarl.europa.eu/doceo/document/LIBE-PR-736469_EN.pdf.

Exchange Network Application (SIENA)[151] as the default system for any exchange between MS LEAs and with Europol outside the scope of the Draft Prüm II Regulation.

2.4. Bilateral Agreements and Reciprocal Courtesy

International cooperation between national LEAs is also regulated by bilateral agreements. In general, such bilateral agreements refer to specific requests that can be submitted and define the procedures and forms of contact as well as the rights and obligations of the requesting and requested states.[152] While bilateral agreements can also specifically address cybercrime as a topic, the extent of existing bilateral agreements actually addressing and adequately governing the particularities of cybercrime investigations remains uncertain.[153] What is certain, however, is that, in the absence of any multilateral or bilateral agreement, international cooperation generally needs to be founded on international courtesy, based on reciprocity.[154]

Traditionally, bilateral agreements on mutual assistance in criminal matters concluded by an individual state are made publicly available in that state's official law gazette. Despite such public availability, a global overview of bilateral agreements seems inhibited by language barriers. In an effort to mitigate at least some of these language barriers to some extent for the purposes of the GRACE project, it was decided to draw on the expertise regarding the 5 Member States selected for the country reports of this Legal Report and elaborate for these an overview of bilateral agreements with non-EU states which currently appear to have gained relevance for the spread of CSEM online.

Europol's annual threat assessments concerning Internet organised crime as well as Europol's regular threat assessments regarding serious and organised crime typically refer to specific countries only, if a particular type of crime appears predominantly linked to that country. Focusing on online CSE, the emerging threat of live distance CSE appears to emanate predominantly from Southeast Asian countries, especially from the **Republic of the Philippines**[155]. However, not all forms of online CSE, especially CSEM circulating online can easily be traced back to a specific country of origin. In fact, once online, any CSEM is available globally and can easily be accessed on all types of devices, including mobile devices. The identification of specific countries where CSEM is mostly accessed or from where CSEM has originated, is significantly impeded not only by the increasing use of anonymisation services[156], but also by the widespread use of encryption tools, including end-to-end

[151] Europol, „Secure Information Exchange Network Application (SIENA)": https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena.

[152] See in this context the UN Model Treaty on Mutual Legal Assistance, 1999, A/RES/45/117.

[153] Gercke, „Understanding Cybercrime: phenomena, challenges and legal response", November 2014, section 6.6.3, p. 267. Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS, 1999, Chapter III, available at: www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

[154] See in this regard: Pop, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, p. 160 et seq.; Stowell, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, p. 262; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976, p. 119.

[155] Europol, Serious and Organised Crime Threat Assessment (SOCTA) 2021, p. 41; Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, p. 39.

[156] Such as Virtual Private Networks (VPNs) or proxy servers: Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023, p. 6.

encrypted apps.[157]

Against this background, a closer analysis of the global hosting patterns for CSEM seems to offer a useful alternative for identifying specific countries relevant for the spread of CSE online. In 2021, the International Association of Internet Hotlines (INHOPE) traced CSEM to 81 countries.[158] Not surprisingly, the only non-EU country to which more than 15 % of the hosted CSEM was traced, was the **United Stated of America (USA)** which has the greatest number of websites available on the internet and where several key market players including Amazon Web Services, Google, LLC, and GoDaddy Operating Company, LLC, have a significant presence. Among the non-EU countries to each of which between 1 – 15 % of the hosted CSEM was traced, are the **Russian Federation**, the **Republic of India** and the **Ukraine**. Below that mark, the non-EU countries to each of which less than 1 % of the hosted CSEM was traced, include (in alphabetical order) **Argentina**, **Chile**, **China**, **Iraq**, **Iran**, **Turkey**, **South Africa** and **Vietnam**. In comparison, about a quarter of the non-EU nationals suspected of participating in organised crime originates from neighbouring countries such as the Western Balkan region, eastern European countries, and North Africa.[159] Further, the map highlighting the main non-EU countries of origin of trafficking victims sexually exploited in the EU (including adults) in Europol's SOCTA 2021 displays a plethora of countries across all continents except Australia. [160]

For cybercrime investigations against the spread of CSEM online, these global hosting patterns seem to indicate an increased need for and relevance of international cooperation with these non-EU countries. This chapter presents for the following 5 Member States an overview of bilateral agreements with these non-EU states: Slovenia (section 2.4.1 below), Cyprus (section 2.4.2 below), Portugal (section 2.4.3 below), Germany (section 2.4.4 below) and Lithuania (section 2.4.5 below). Each overview of national bilateral agreements is not intended to be a comprehensive analysis. Rather, each overview identifies applicable multilateral or bilateral agreements governing mutual assistance in criminal matters with the selected non-EU states and indicates whether and to what extent they contain provisions specifically dedicated to cybercrime investigations in general or investigations of online CSE cases in particular.

2.4.1. Bilateral Agreements in Slovenia

States often conclude multilateral and bilateral international treaties with the aim of facilitating and improving cooperation between judicial authorities in civil and criminal matters.[161]

The published lists of multilateral and bilateral international agreements are of an informative nature, as the Republic of Slovenia is bound in relation to other countries only by international agreements in the form and content, as derived from their official publication in official gazettes.

The Ministry of Justice of Republic of Slovenia publishes international treaties that regulate the field of international legal assistance in digital form, which enables a more transparent, easier and more efficient search for legal information regarding the enforcement of citizens' rights in cross-border proceedings, as well

[157] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023, p. 6; Europol, Serious and Organised Crime Threat Assessment (SOCTA) 2021, p. 41.
[158] INHOPE Association, Annual Report 2021, p. 39.
[159] Europol, Serious and Organised Crime Threat Assessment (SOCTA) 2021, p. 19.
[160] Europol, Serious and Organised Crime Threat Assessment (SOCTA) 2021, p. 71.
[161] While Anton Toni Klančnik, MA (Europol) made only a general introduction at this point taking all five introductory paragraphs of this section from official website of the Ministry of Justice of the Republic of Slovenia (https://www.gov.si/teme/mednarodno-sodelovanje-v-pravosodju/), he wrote the subsections.

as international legal assistance and the international operations of economic entities.

The former Yugoslavia (the SFRY and its predecessors) has concluded bilateral agreements with some other countries that regulate the cumulative or alternative field of international legal assistance in civil matters and international legal assistance in criminal matters. After the independence of the Republic of Slovenia, the aforementioned agreements were applied on the territory of the Republic of Slovenia on the basis of Article 3 of the Constitutional Act for the Implementation of the Fundamental Constitutional Document on Independence and Independence of the Republic of Slovenia (Official Gazette of the Republic of Slovenia, No. 1/91) in connection with Article 1 of the Constitutional Act on implementation of the Constitution of the Republic of Slovenia (Official Gazette of the Republic of Slovenia, No. 33/91). By adopting acts on the succession of agreements, the Republic of Slovenia has already notified the succession of some bilateral agreements concluded by the former Yugoslavia, and the rest are applied on the basis of the aforementioned constitutional law until a different agreement is reached with each contracting state. Also, after gaining independence, the Republic of Slovenia concluded bilateral agreements with some countries. At the same time, it should be noted that bilateral agreements can be used in relation to the member states of the European Union, if there is no legal act of the European Union in force for an individual area or legal institute, which specifically defines the relationship to bilateral agreements. As regards the use of bilateral agreements with countries with which the Republic of Slovenia has concluded international agreements that regulate the same field or legal institutes, international agreements in principle determine the relationship to bilateral agreements and the manner of their application.

Multilateral international treaties or international agreements bind countries that become contracting states after signing an individual treaty and the ratification process or accession to an international treaty. International agreements in the field of judicial cooperation in criminal matters regulate cooperation between the competent judicial authorities of the contracting states. Such cooperation most often covers the field of extraditions, transfer of execution of sentences and international legal assistance in criminal matters (service, collection of evidence, resignation of criminal prosecution, etc.).

2.4.1.1. Republic of Slovenia: Domestic (National) Legislation

There are several legal grounds for international cooperation in Slovenia among the law enforcement authorities and among other criminal justice authorities, such as prosecution's office and judiciary. Numerous bilateral and international treaties are presented as addition to this section.

Presented is relevant legal framework in relation to criminal matters:

2.4.1.1.1. Law Enforcement Authority

The Slovenian Police is a body within the Ministry of the Interior. It has gained independence, whereby the ministry determines the development, organizational, personnel and other fundamental directions for its work, takes care of its financial operations and investments, and coordinates and harmonizes the police information and telecommunications system with the systems of other state bodies. The Ministry also directs and supervises the implementation of police duties. The headquarters of the Police is in Ljubljana, capitol city. It operates at three levels: national, regional and local. Organizationally, it consists of the General Police Directorate (national), 8 Police Directorates (regional) and 111 police stations (local).

The Slovenian Police is the only police force in the country. The relevant law for the LEA in Slovenia is actually

Police Tasks And Powers Act (orig. Zakon o nalogah in pooblastilih Policije, hereinafter the official abbreviation will be used – ZNPPol), through which the international cooperation among law enforcement authorities, foreign authorities and different international organization is defined. Additional legal basis is enshrined in the Organisation and Work of the Police Act (orig. Zakon o organiziranosti in delu v policiji, hereinafter the official abbreviation will be used – ZODPol),

The Article 117 of ZNPPol provides the legal basis for transferring of personal data to foreign authorities and international organizations. It defines that this activity is carried out based on the provisions of the relevant international treaty, legal act or decisions of an international organization, or according to the provisions of the laws by which these legal acts or decisions are implemented. Yet, this is possible based of an international agreement, by which the Republic of Slovenia has transferred the exercise of sovereign rights to them, as well as the transfer of personal data to EU MS or to the EEA. The legal clause provides a condition. It says, if necessary for the exercise of police powers, the police may, at their request or on their own initiative, by subject to the condition of actual reciprocity forward the collected personal and other data. The police may mark certain personal data as sensitive and limit the purpose of their processing. Additional legal provisions are collected under chapter VI of the ZODPol, that provides a legal basis for international cooperation and cooperation in international civil missions through its police duties on the basis of accepted international obligations that bind the Republic of Slovenia.

2.4.1.1.2. Mutual Legal Assistance in Criminal Matters

International criminal legal assistance is provided according to the provisions of Criminal Procedures Act (orig. Zakon o kazenskem postopku, hereinafter the official abbreviation will be used – ZKP), unless otherwise stipulated by an international treaty or law. Under legal basis for such cooperation is based per Cooperation in Criminal Matters with the Member States of the European Union Act (orig. Zakon o sodelovanju v kazenskih zadevah z državami članicami Evropske unije, hereinafter the official abbreviation will be used – ZSKZDČEU-1), which stipulates the procedures for cooperation in criminal matters with the competent national authorities and authorities in other EU MSs.

The cooperation in criminal matters includes:

1. mutual recognition and enforcement of decisions of judicial authorities, courts and other competent authorities;
2. resignation and taking over of criminal prosecution;
3. legal assistance in criminal matters, including the establishment of joint investigative teams and the joint implementation of investigative measures;
4. other forms of cooperation in accordance with the legal regulation in the European Union and its member states.

In regard to the mutual recognition and enforcement of decisions, those encompass:

- for the arrest and surrender of persons, seizure and confiscation of objects, temporary securing of claims for confiscation of property benefits and confiscation of property benefits,
- issuing or confirming a European investigation warrant,
- imposing prison sentences, security measures and other measures related to deprivation of liberty,
- imposing measures to ensure the defendant's presence and the successful execution of criminal proceedings,

- by which conditional sentences with protective supervision, conditional suspensions of sentencing, alternative sanctions and decisions on conditional release with protective supervision are pronounced,
- issuing a European protection order and
- imposing monetary sanctions.

Provisions under the ZKP are collected under the Chapter XXX – Procedure for international legal assistance and enforcement of international agreements in criminal matters and under the Chapter XXXI – Procedure for extradition of debtors and convicted persons. These chapters are more or less truncated, as the provisions were covered in the aforementioned newer legislation (ZSKZDČEU-1), however, both laws must be considered mutually.

The ZSKZDČEU-1 provides for the mutual recognition and enforcement of decisions of judicial authorities for the arrest and surrender of persons, seizure and confiscation of objects, temporary securing of claims for confiscation of property benefit and deprivation of property benefit, decisions of courts or other competent authorities issuing a European investigation warrant, court decisions, with which prison sentences, security measures and other measures related to deprivation of liberty are imposed, court decisions with which measures are imposed to ensure the defendant's presence and for the successful execution of criminal proceedings, court decisions or competent authorities with which conditional sentences are imposed with protective supervision, conditional suspensions of sentencing, alternative sanctions and decisions on parole with protective supervision, decisions of courts or competent authorities issuing a European protection order, decisions of competent authorities imposing monetary sanctions, establishment of joint investigative teams and total from implementation of investigative measures, exchange of data from criminal records and cooperation with Eurojust and the European Judicial Network.

As addition, through this act Republic of Slovenia has implemented numerous[162] legal acts of the European Union.

2.4.1.2. Succession by Republic of Slovenia after the former SFR Yugoslavia

Yugoslavia is the collective name of several countries of South (orig. Jug) Slavic (orig. Slovani) nations in the territory of the north-western Balkans between 1918 and 2003. It existed on the territory of nowadays of the following states: Bosnia and Herzegovina, Montenegro, Croatia, Kosovo[163], North Macedonia, Slovenia and Serbia. It existed for most of the 20th century (1918–1992) under different names and political arrangements:

- State of Slovenes, Croats and Serbs (orig. Država SHS), 29 October 1918 – 1 December 1918;
- Kingdom of Serbs, Croats and Slovenes, 1 December 1918 – 3 October 1929;
- Kingdom of Yugoslavia, 3 October 1929 – formally abolished after the 2WW;
- Democratic Federative Yugoslavia - DFJ (new Yugoslavia), 10 August 1945 – 29 November 1945;

[162] It is an extensive list of legal acts, but it would go beyond the purpose of their publication in this section. Let us point out that the full list is provided by the Article 2 of the ZSKZDČEU-1.

[163] This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

- Federative People's Republic of Yugoslavia (FLRJ) 29 November 1945 – 7 April 1963;
- Socialist Federal Republic of Yugoslavia (SFRJ), 7 April 1963 – during 25 June 1991 and 27 April 1992;
- Slovenia declared its independence on 25 June 1991;[164]
- Federal Republic of Yugoslavia - 27 April 27 1992 – 4 February 2003.

Brief historical overview will help reader to understand the legal aspects of succession regarding Republic of Slovenia after Yugoslavia was abolished. In this regard, acts notifying succession to agreements between the former Yugoslavia and other countries, related and limited only to different criminal matters[165,166] are listed below. It is important to highlight that firstly is presented a main act on succession and then the details of concrete historical act is presented that is kept valid after succession. Taking into account the mentioned conditions, the agreements are valid with the following countries:

- **Russian Federation**, date of acceptance: 05/04/2011, Act on succession to agreements between the former Yugoslavia and the Union of Soviet Socialist Republics that shall remain in force between the Republic of Slovenia and the Russian Federation, EIF: 14/04/2001, Act no. 3. Treaty between the Federal People's Republic of Yugoslavia and the Union of Soviet Socialist Republics on legal assistance in civil, family and criminal matters, Moscow, 24/02/1962 [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije z Zvezo sovjetskih socialističnih republik, ki naj ostanejo v veljavi med Republiko Slovenijo in Rusko federacijo, Akt št. 3. Pogodba med Federativno ljudsko republiko Jugoslavijo in Zvezo sovjetskih socialističnih republik o pravni pomoči v civilnih, družinskih in kazenskih zadevah, Moskva, 24. 2. 1962*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2001-02-0023?sop=2001-02-0023;
- **Cyprus**, date of acceptance: 29/02/2000, Act on succession to agreements between the former Yugoslavia and Republic of Cyprus that shall remain in force between the Republic of Slovenia and the Republic of Cyprus, EIF: 11/03/2000, Act no. 9. Agreement between the SFRY and the Republic of Cyprus on legal assistance in civil and criminal matters, Nicosia, 19 September 1984, [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije z Republiko Ciper, ki naj ostanejo v veljavi med Republiko Slovenijo in Republiko Ciper, Akt št. 9. Pogodba med SFRJ in Republiko Ciper o pravni pomoči v civilnih in kazenskih zadevah, Nikozija, 19. 9. 1984*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2000-02-0017?sop=2000-02-0017;
- **Poland**, date of acceptance: 20/06/1994, Act on succession to agreements between the former Yugoslavia and Poland, EIF: 14/07/1994, Act no. 9 - Treaty between the FLRJ and the Republic of Poland on legal transactions in civil and criminal matters, Warsaw, 6 February 1960, [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije s Poljsko, Akt št. 9 - Pogodba med FLRJ in LR Poljsko o pravnem prometu v civilnih in kazenskih zadevah, Varšava, 6. 2. 1960*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0058?sop=1994-02-0058;
- **Germany**, date of acceptance: 22/11/1993, Act on succession to agreements between the former Yugoslavia and the Federal Republic of Germany, EIF: 18/12/1993, Act no. 21. Agreement between

[164] Slovenia, officially the Republic of Slovenia, is a European country with a geographical location in the extreme north of the Mediterranean and in the extreme south of Central Europe. Slovenia borders Italy to the west, Austria to the north, Hungary to the northeast, and Croatia to the east and south. The capital city is Ljubljana, which is the economic, cultural and political centre.

[165] Underlined by Anton Toni Klančnik, MA (Europol).

[166] Anton Toni Klančnik, MA (Europol) avoided making the list of the agreements on administration, taxes, consular, trade and other matters that are not directly related to criminal matters.

the Socialist Federal Republic of Yugoslavia and the Federal Republic of Germany on extradition dated 26 November 1970, and Act no. 22. Treaty between the Socialist Federal Republic of Yugoslavia and the Federal Republic of Germany on legal assistance in criminal matters of 1 October 1971 [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije z Zvezno republiko Nemčijo, Akt št. 21. Sporazum med Socialistično federativno republiko Jugoslavijo in Zvezno republiko Nemčijo o izročitvi z dne 26 November 1970, objavljen v Uradnem listu SFRJ -Mednarodne pogodbe, št. 17/76; in Akt št. 22. Pogodba med Socialistično federativno republiko Jugoslavijo in Zvezno republiko Nemčijo o pravni pomoči v kazenskih stvareh z dne 01/10/1971*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1993-02-0092?sop=1993-02-0092;

- **Italy**, date of acceptance: 29/07/1992, Act notifying succession to agreements between the former Yugoslavia and the Italian Republic, EIF: 15/08/1992, Act no. 1. Convention between the Kingdom of SHS and Italy on the extradition of the guilty, dated 6 April 1922, [orig. *Akt o notifikaciji nasledstva sporazumov nekdanje Jugoslavije z Republiko Italijo, Akt št. 1. Konvencija med Kraljevino SHS in Italijo o izročanju krivcev, z dne 6. 4. 1922*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1992-02-0060?sop=1992-02-0060;
- **Turkey**, Date of acceptance: 02/03/2001, Act on succession to agreements between the former Yugoslavia and the Republic of Turkey that shall remain in force between the Republic of Slovenia and the Republic of Turkey, EIF: 17/03/2001, Act no. 15 - Convention between the SFRY and the Republic of Turkey on judicial legal assistance in criminal matters, Ankara, 8 October 1973, and Act no. 19 - Agreement between the SFRY and the Republic of Turkey on mutual surrender of convicts serving prison sentences, Belgrade, 22 June 1989, [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije z Republiko Turčijo, ki naj ostanejo v veljavi med Republiko Slovenijo in Republiko Turčijo, Akt št. 15 - Konvencija med SFRJ in Republiko Turčijo o sodni pravni pomoči v kazenskih zadevah, Ankara, 8. 10. 1973, in Akt št. 19 - Pogodba med SFRJ in Republiko Turčijo o medsebojni predaji obsojencev zaradi prestajanja kazni zapora, Beograd, 22. 6. 1989*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2001-02-0015?sop=2001-02-0015;
- **Czech Republic**, Date of acceptance: 24/05/1994 , Act on succession to agreements between the former Yugoslavia and the former Republic of Czechoslovakia that shall remain in force between the Republic of Slovenia and the Czech Republic, EIF: 18/06/1994, Act no. 4 - Agreement between SFR Yugoslavia and the Czechoslovak Socialist Republic on the Regulation of Legal Relations in Civil, Family and Criminal Matters, Belgrade, 20 January 1964; and Act No. 7 - Treaty between the SFRY and the Czechoslovakia on the mutual extradition of convicted persons for serving a prison sentence, Prague, 23 May 1989, [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije z nekdanjo Češko in Slovaško federativno republiko, ki naj veljajo med Republiko Slovenijo in Češko republiko, Akt št. 4 - Pogodba med SFR Jugoslavijo in Češkoslovaško socialistično republiko o urejanju pravnih odnosov v civilnih, rodbinskih in kazenskih zadevah, Beograd, 20. 1. 1964; in Akt št.7 - Pogodba med SFRJ in ČSSR o medsebojni izročitvi obsojenih oseb zaradi prestajanja kazni zapora, Praga, 23. 5. 1989*]; https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0045?sop=1994-02-0045
- **Slovakia**, see the same as Czech Republic,
- **Belgium**, date of acceptance: 26/06/1996, Act on succession to agreements between the former Yugoslavia and the Kingdom of Belgium that shall remain in force between the Republic of Slovenia and the Kingdom of Belgium, EIF: 12/07/1997, Act no. 9 - Convention between the SFRY and the Kingdom of Belgium on extradition and legal assistance in criminal matters, Belgrade, 4 June 1971, [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije s Kraljevino Belgijo, ki naj ostanejo v veljavi med Republiko Slovenijo in Kraljevino Belgijo, Akt št. 9 - Konvencija med SFRJ in Kraljevino Belgijo o izročitvi in pravni pomoči v kazenskih zadevah, Beograd, 4. 6. 1971*],

- **New Zealand**, date of acceptance: 29/01/2004, Act on succession to agreements between the former Yugoslavia and New Zealand that shall remain in force between the Republic of Slovenia and New Zealand, EIF: 13/02/2004, Act no. 1 - Treaty between Serbia and Great Britain on mutual extradition of criminals, Belgrade, 6 December 1900, [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije z Novo Zelandijo, ki naj ostanejo v veljavi med Republiko Slovenijo in Novo Zelandijo, Akt št. 1 - Pogodba med Srbijo in Veliko Britanijo o medsebojnem izročanju storilcev kaznivih dejanj, Beograd, 6. 12. 1900*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0012?sop=2004-02-0012;
- **Australia**, date of acceptance: 28/10/1997, Act on the succession of agreements between the former Yugoslavia and Australia, which should remain in force between the Republic of Slovenia and Australia, EIF: 08/11/1997, act no. 1 - Treaty between Serbia and Great Britain on mutual extradition of criminals, 6 December 1900 [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije z Avstralijo, ki naj ostanejo v veljavi med Republiko Slovenijo in Avstralijo, akt št. 1 - Pogodba med Srbijo in Veliko Britanijo o medsebojnem izročanju storilcev kaznivih dejanj, 6. 12. 1900*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1997-02-0065?sop=1997-02-0065;
- **France**, date of acceptance: 24/05/1994, Act on succession to agreements between the former Yugoslavia and the French Republic that shall remain in force between the Republic of Slovenia and the French Republic, EIF: 18/06/1994, Act under no. 4 - Convention between Yugoslavia and France on mutual legal assistance in criminal matters, signed on October 29, 1969; and Act under no. 5 - Convention on Extradition between the Governments of Yugoslavia and France; signed on 23 September 1970 [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije z Republiko Francijo, ki naj veljajo med Republiko Slovenijo in Republiko Francijo, akt št. 4 - Konvencija med Jugoslavijo in Francijo o vzajemni pravni pomoči v kazenskih zadevah, podpisana 29. 10. 1969; in akt št 5 - Konvencija o izročitvi med vladama Jugoslavije in Francije; podpisana 23. 9. 1970*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0044?sop=1994-02-0044
- **Spain**, date of acceptance: 26/01/1996, Act on succession to agreements between the former Yugoslavia and the Kingdom of Spain that shall remain in force between the Republic of Slovenia and the Kingdom of Spain, EIF: 13/02/1996, act under no. 5 - Agreement between the SFRY and Spain on legal assistance in criminal matters and extradition, Belgrade, 8 July 1980, [orig. *Akt o nasledstvu sporazumov nekdanje Jugoslavije s Kraljevino Španijo, ki naj ostanejo v veljavi med Republiko Slovenijo in Kraljevino Španijo, akt št. 5 - Pogodba med SFRJ in Španijo o pravni pomoči v kazenskih stvareh in izročitvi, Beograd, 8. 7. 1980*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1996-02-0002?sop=1996-02-0002;
- **USA**, date of acceptance: 29/09/2020, Act on succession to agreements between the former Yugoslavia and the United States of America that shall remain in force between the Republic of Slovenia and the United States of America, EIF: 24/10/2020, act under no. 2 – Extradition Treaty between the Kingdom of Serbia and the United States of America, [orig. *Akt o notifikaciji nasledstva sporazumov nekdanje Jugoslavije z Združenimi državami Amerike, ki ostajajo v veljavi med Republiko Slovenijo in Združenimi državami Amerike (MNNSNJ), akt št. 2 - Pogodba o izročitvi med Kraljevino Srbijo in Združenimi državami Amerike*], https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2020-02-0019?sop=2020-02-0019.

As addition, below are the two lists on concrete examples of (legal) bilateral cooperation, based on Slovenia's agreements with other countries and focused on criminal matters. The orange list in Table 1 is about the bilateral agreements on the country to country level, while the blue list in Table 2 is about bilateral agreement on the law enforcement level.

Table 1 – Orange list: Bilateral agreement on the country to country level

No.	Country	Bilateral Agreement (country to country level)
1.	**Albania**	Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Albania on the cooperation in combating terrorism, illicit traffic in drugs and organised crime, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO588
	Austria	Act Ratifying the Agreement between the Ministry of the Interior of the Republic of Slovenia and the Federal Minister of the Interior of the Republic of Austria on the cooperation in the suppression of international organised crime, international illicit drug traffic and international terrorism, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1996-02-0017?sop=1996-02-0017 Act Ratifying the Agreement between the Republic of Slovenia and the Republic of Austria on Police Cooperation, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052?sop=2004-02-0052 Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Austria on the acceptance of persons at the common border and the agreement for the implementation of the agreement between the Government of the Republic of Slovenia and the Government of the Republic of Austria on the acceptance of persons at the common border, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1993-02-0026?sop=1993-02-0026
	Belgium	Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Kingdom of Belgium on police cooperation, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2001-02-0042?sop=2001-02-0042
	Benelux (Belgium, Luxembourg, Netherlands)	Act Ratifying the Agreement between the Government of the Republic of Slovenia, on the one hand, and the governments of the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands, on the other, on the acceptance of persons whose entry or stay is contrary to existing regulations, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1993-02-0021?sop=1993-02-0021
	Bulgaria	Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Bulgaria on Co-operation in the fight against organised crime, illicit drugs, psychotropic substances and precursors trafficking, terrorism and other serious crimes, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2002-02-0024?sop=2002-02-0024
	Bosnia and Herzegovina	Act Ratifying the Treaty between the Republic of Slovenia and Bosnia and Herzegovina on Extradition, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2002-02-0096?sop=2002-02-0096

		Act Ratifying the Treaty between the Republic of Slovenia and Bosnia and Herzegovina on Mutual Enforcement of Judgments in Criminal Matters, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2002-02-0095?sop=2002-02-0095 Act ratifying the Agreement between the Republic of Slovenia and Bosnia and Herzegovina on legal assistance in civil and criminal matters, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2010-02-0089?sop=2010-02-0089 Act ratifying the Agreement between the Government of the Republic of Slovenia and the Council of Ministers of Bosnia and Hercegovina on the Readmission of Persons whose Residence is Illegal, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0034?sop=2007-02-0034
	Cyprus	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Cyprus concerning the co-operation in the fight against terrorism, illicit drug trafficking and organized crime, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0093?sop=2003-02-0093
	Czech Republic	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Czech Republic on the reception of persons at the state border, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1999-02-0027?sop=1999-02-0027 Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Czech Republic on cooperation in the suppression of illicit traffic in drugs and psychotropic substances and against organized crime and in the fight against terrorism, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1999-02-0028?sop=1999-02-0028
	Montenegro	Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Montenegro on cooperation in the fight against organised crime, people trafficking and illegal migrations, trafficking in illicit drugs and precursors, terrorism and other crimes, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0050?sop=2007-02-0050
	Denmark	Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Kingdom of Denmark on the readmission of citizens of one of the two countries and foreigners illegally staying on the territory of the other country, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1997-02-0056?sop=1997-02-0056
	Estonia	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Estonia on co-operation in the

		fight against organised crime, illicit drugs, psychotropic substances and precursors trafficking and terrorism, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0006?sop=2004-02-0006
	France	Act Ratifying the Agreement on Cooperation in the Field of Internal Security between the Government of the Republic of Slovenia and the Government of the French Republic, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2008-02-0037?sop=2008-02-0037 Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of France on the acceptance of persons whose entry or stay is contrary to the applicable regulations, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1993-02-0076?sop=1993-02-0076
	Greece	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Hellenic Republic on cooperation in fighting crime, especially terrorism, illicit drug trafficking and organized crime, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0095?sop=2003-02-0095 Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Hellenic Republic on the readmission of persons in an irregular situation, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1995-02-0028?sop=1995-02-0028
	Croatia	Act Ratifying the Agreement between the Republic of Slovenia and the Republic of Croatia on Cross-border police co-operation, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Croatia on the readmission of persons whose entry or residence is illegal, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2006-02-0040?sop=2006-02-0040 Act ratifying the Agreement between the Republic of Slovenia and Republic of Croatia on mutual enforcement of court decisions in criminal matters, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0062?sop=1994-02-0062 Act on Ratification of the Treaty between the Republic of Slovenia and the Republic of Croatia on Legal Aid in Civil and Criminal Matters, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0063?sop=1994-02-0063

		Act ratifying the Agreement between the Republic of Slovenia and Republic of Croatia on extradition, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1995-02-0011?sop=1995-02-0011 and https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1995-02-0070?sop=1995-02-0070 Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Croatia on the readmission of persons at State border and the Protocol on the application of the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Croatia on the readmission of persons at State border, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0023?sop=1994-02-0023 Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Croatia on the cooperation in combating terrorism, illicit traffic in and abuse of drugs as well as against organised crime, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0022?sop=1994-02-0022
	Italy	Act on the ratification of the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Italy on the acceptance of persons at the state border, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1997-02-0041?sop=1997-02-0041 Act on the ratification of the agreement on cooperation between the Ministry of the Interior of the Republic of Slovenia and the Ministry of the Interior of the Republic of Italy in the fight against illegal trade in narcotic and psychotropic substances and against organized crime and the minutes of the meeting between the Ministry of the Interior of the Republic of Slovenia and the Ministry of the Interior of the Republic of Italy on the exchange of computerized information relating to the illegal trade in narcotic and psychotropic substances along the Balkan route and in the Mediterranean, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0016?sop=1994-02-0016 and https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1995-02-0022?sop=1995-02-0022 Act on the ratification of the Agreement between the Government of the Republic of Slovenia and the Government of the Italian Republic on police cooperation, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1999-02-0097?sop=1999-02-0097 Act Ratifying the Agreement between the Republic of Slovenia and the Republic of Italy on cross-border police cooperation, https://www.uradni-list.si/glasilo-

		uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134
	Canada	Act Ratifying the Arrangement between the Government of Canada and the Government of the Republic of Slovenia on the mutual removal of the citizens of both countries whose entry or residence in the territory of the other country are illegal, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1996-02-0003?sop=1996-02-0003 Act Ratifying the Arrangement between the Government of Canada and the Government of the Republic of Slovenia on the mutual cooperation the prevention of illegal migration, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1996-02-0004?sop=1996-02-0004
	Kosovo	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Kosovo on the Admission of Persons Residing without Authorisation and the Protocol between the Government of the Republic of Slovenia and the Government of the Republic of Kosovo on the Implementation of the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Kosovo on the Admission of Persons Residing without Authorisation, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2011-02-0091?sop=2011-02-0091 Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Kosovo on police cooperation, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2015-02-0067?sop=2015-02-0067
	Latvia	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Latvia on co-operation in combating terrorism, organized crime, illicit trafficking in narcotic drugs, psychotropic substances and precursors and other serious crimes, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2006-02-0039?sop=2006-02-0039
	Lithuania	Act on the ratification of the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Lithuania on the readmission of persons whose entry into the country or stay in it is contrary to the applicable regulations of the country, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1997-02-0012?sop=1997-02-0012
	Hungary	Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Hungary on the readmission, at the State border, of persons staying illegally in the other State's territory, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1999-02-0030?sop=1999-02-0030 Act Ratifying the Agreement between the Republic of Slovenia and the Republic

		of Hungary on cross-border co-operation of law enforcement authorities, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Hungary on the cooperation in combating terrorism, illicit traffic in drugs and organised crime, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0005?sop=1994-02-0005
	North Macedonia	Act on the Ratification of the Treaty between the Republic of Slovenia and the Republic of Macedonia on Extradition, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1997-02-0044?sop=1997-02-0044 Act on the ratification of the Treaty between the Republic of Slovenia and the Republic of Macedonia on legal assistance in civil and criminal matters, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1997-02-0046?sop=1997-02-0046 Act on the Ratification of the Treaty between the Republic of Slovenia and the Republic of Macedonia on Mutual Enforcement of Court Decisions in Criminal Matters, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1997-02-0045?sop=1997-02-0045 Act on the ratification of the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Macedonia on the readmission of persons whose entry into the country and/or stay in it is contrary to internal law, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1998-02-0044?sop=1998-02-0044 Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Macedonia on the cooperation in combating terrorism, illicit traffic in drugs and organised crime, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0093?sop=1994-02-0093
	Malta	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of Malta on co-operation in the fight against organised crime, trafficking in illicit drugs, psychotropic substances and precursors, terrorism and other serious crimes, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0094?sop=2003-02-0094

	Germany	Act on the ratification of the Agreement between the Government of the Republic of Slovenia and the Government of the Federal Republic of Germany on cooperation in the suppression of serious crimes, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2001-02-0043?sop=2001-02-0043 Agreement between the Govrnment of the Republic of Slovenia and the Federal Government of the Federal Republic of Yugoslavia on co-opertion in the fight against organised crime, illicit drugs, psychotropic substances and precursors tafficiking, terrorism and other serious crimes, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2001-02-0044?sop=2001-02-0044 Agreement between the Government of the Republic of Slovenia and the Federal Government of the Federal Republic of Yugoslavia on return and readmission of persons who do not comply with the conditions for entry of stay on the territory of the other state, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2001-02-0045?sop=2001-02-0045
	Poland	Act on the ratification of the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Poland on cooperation in the fight against terrorism, organized crime and illegal trafficking in drugs, psychotropic substances and precursors, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1997-02-0011?sop=1997-02-0011
	Serbia	Act ratifying the Treaty between the Republic of Slovenia and the Republic of Serbia on Extradition, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6700 Act ratifying the Treaty between the Republic of Slovenia and the Republic of Serbia on the mutual enforcement of judgments in criminal matters, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6790 Act ratifying the Treaty between the Republic of Slovenia and the Republic of Serbia on legal assistance in civil and criminal matters, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6701
	Sweden	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Kingdom of Sweden on Cooperation in the Fight against Organised Crime, Illicit Drug Trafficking in Drugs and Precursors, Terrorism and other Serious Crimes, http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED3533
	Switzerland	Act ratifying the Agreement between the Republic of Slovenia and the Swiss Confederation on Cooperation in the Fight against Crime and the Protocol between the Government of the Republic of Slovenia and the Federal Council of the Swiss Confederation on Secondment of Liaison Officers, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4341

	Turkey	Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Turkey on Co-operation in the Fight against Organised Crime, Illicit Drugs Trafficking, International Terrorism and other Serious Crimes, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4382
	Ukraine	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Cabinet of Ministers of Ukraine on Cooperation in the Fight against Crime, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6273
	United States of America	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the United States of America On Enhancing Cooperation in Preventing and Combating Serious Crime, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6546 Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the United States of America on the instrument as referred to in third paragraph of Article 3 of the Agreement on Mutual Legal Assistance between the European Union and the United States of America, signed at Washington on 25 June 2003, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4574 Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the United States of America on the instrument as referred to in the second paragraph of Article 3 of the Agreement on Extradition between the European Union and the United States of America signed on 25 June 2003, on the application of the Treaty on Extradition between the Kingdom of Serbia and the United States, signed on 25 October 1901, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4575

Table 2 – Blue list: Bilateral agreement on the Law Enforcement level

No.	Country	Bilateral Agreement (law enforcement level)
	Austria	Decree ratifying the Arrangement between the Government of the Italian Republic and the Federal Government of the Republic of Austria and the Government of the Republic of Slovenia on Cooperation in the police centre Vrata – Megvarje, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2005-02-0008?sop=2005-02-0008
	Italy	Decree ratifying the Memorandum on the cooperation between the Police of the Republic of Slovenia and the Police of the Italian Republic, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1997-02-0072?sop=1997-02-0072
	Croatia	Decree ratifying the Protocol between the Ministry of the interior of the Republic of Slovenia and the Ministry of the Interior of the Republic of Croatia concerning the implementation of the Agreement between the

		Government of the Republic of Slovenia and the Government of the Republic of Croatia on the readmission of persons whose entry or residence is illegal, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2006-02-0042?sop=2006-02-0042
	Czech Republic	Decree Ratifying the Protocol between the Ministry of the Interior of the Republic of Slovenia and the Ministry of the Interior of the Czech Republic for the Implementation of the Agreement between the Government of the Republic of Slovenia and the Government of the Czech Republic on the Readmission of Persons at the State Border, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0079?sop=2003-02-0079
	Poland	Decree Ratifying the Protocol between the Ministry of the Interior of the Republic of Slovenia and the Minister of the Interior and the Administration of the Republic of Poland on the Implementation of the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Poland on the Readmission of Persons without a Residence Permit, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2006-02-0134?sop=2006-02-0134
	Slovakia	Decree Ratifying the Protocol on the implementation of the Agreement between the Government of the Slovak Republic and the Government of the Republic of Slovenia on the reception of persons at the state border, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2000-02-0006?sop=2000-02-0006
	Serbia (FR Yugoslavia)	Decree ratifying the Protocol for the Implementation of the Agreement between the Government of the Republic of Slovenia and the Federal Government of the Federal Republic of Yugoslavia on return and readmission of Persons that do not comply with the conditions for the entry or stay on the territory of the other state, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2001-02-0075?sop=2001-02-0075
	Serbia	Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Serbia on Police Cooperation, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6561
	Bosnia and Herzegovina	Decree ratifying the Agreement between the Government of the Republic of Slovenia and the Council of Ministers of Bosnia and Hercegovina on Police Cooperation, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0049?sop=2007-02-0049

Finally, Slovenia has also several agreements on cross-border control and related border activities with countries, such as Austria, Italy, Hungary, Croatia, Bosnia and Herzegovina, and Poland. On the 1st May 2005, the Agreement between the Government of the Italian Republic, the Government of the Federal Republic of Austria and the Government of the Republic of Slovenia on cooperation in the police center in Vrata –

Megvarje[167] (orig. Dogovor o sodelovanju v policijskem centru v Vratih – Megvarje), signed on 14 September 2004, has entered into force for Slovenia.

2.4.2. Bilateral Agreements in Cyprus

Mutual assistance in criminal matters between Cyprus and foreign states, i.e., non-EU Member States is governed by bilateral and multilateral Agreements. As far as mutual assistance with EU Member States is concerned, this is governed by the 2001 European Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union coupled with Directive 2014/41/EU regarding the European Investigation Order in criminal matters which has replaced several of the provisions of said Convention. All bilateral and multilateral agreements between Cyprus and other countries are published in related lists on the website of the Cyprus Ministry of Justice and Public Order,[168] though a more comprehensive list of the bilateral agreements by reference to each country can be found on the website of the Office of the Law Commissioner.[169]

More specifically, apart from some bilateral agreements governing specific matters, such as extradition and the transfer of sentenced persons, Cyprus has concluded bilateral agreements governing mutual assistance in among others[170] criminal matters with Syria,[171] Egypt,[172] China,[173] the USA[174] and Libya.[175] Similar bilateral agreements were also concluded with the Soviet Union and Yugoslavia before their dissolution.[176] As far as Russia is concerned, there is also in a place a Memorandum of Co-operation between the Ministries of Justice of the two countries (Russia and Cyprus).[177] All these bilateral agreements (and the same holds true of multilateral agreements) are ratified through national law passed specifically for this purpose and in this way, they become part of the national legal order. None of the aforementioned bilateral agreements between Cyprus and non-EU countries on mutual assistance contains provisions specifically dedicated to *cybercrime* investigations in general or investigations of *online CSE cases* in particular.

Other bilateral agreements with non-EU states also exist, yet those focus on specific crimes[178] and their

---

[167] Available at: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2005-22-0004?sop=2005-22-0004.

[168] http://www.mjpo.gov.cy/MJPO/mjpo.nsf/All/97349719B6FCBC9CC22584E30046B887?OpenDocument.

[169] http://www.olc.gov.cy/olc/olc.nsf/All/5127B9EF26EA434EC225847300280E1F/$file/Bilateral0817.pdf.

[170] Most mutual assistance bilateral agreements govern mutual assistance in other matters too, such as civil and/or commercial matters.

[171] Law 160/86 as amended by 13(III)/97.

[172] Law 32(III)/92 as amended by 14(III)/96.

[173] Law 19(III)/95.

[174] Law 20(III)/2002 (this one focuses on criminal matters only).

[175] Law 32(III)/2005.

[176] Law 172/86 and Law 179/86 respectively. Several of the countries that were part of the former Soviet Union, such as Russian, Ukraine and Georgia exchanged notes or entered into protocolos ratified by law confirming their continued committement by the provisions of said bilateral agreements.

[177] The content of said Memorandum has not been found online.

[178] The Agreement between the Government of the Republic of Cyprus and the Government of the Republic of India on Combating International Terrorism, Organised Crime and Illicit Drug Trafficking Nicosia, 25 May 2007 and Agreement between the Government of the Republic of Cyprus and the Government of the State of Israel on Cooperation in Combating Illicit Trafficking and Abuse of Narcotic Drugs and Psychotropic Substances, and Terrorism and Other Serious Crimes are a couple of examples.

provisions, even when tackling mutual assistance and/or international co-operation could not be regarded as specifically dedicated to *cybercrime* investigations in general or investigations of *online CSE cases* in particular. The same is true of bilateral agreements such as the Agreement between Government of the Republic of Cyprus and the Cabinet of Ministers of Ukraine on Co-operation in Crime Combating as cybercrime and CSE are not mentioned in said agreement.[179]

Cyprus is also a party to several multilateral agreements; these however do not cover mutual assistance in criminal matters in general. Rather, they focus on more specific criminal matters, such as the fight against the international organised crime,[180] against corruption[181] or for the suppression of terrorist bombings.[182] Again none of these multilateral agreements contains provisions specifically dedicated to *cybercrime* investigations in general or investigations of *online CSE cases* in particular, though they may contain provisions on international co-operation. Cyprus is also a party to the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959 which has been ratified or acceded by a number of non-EU member states and which remains applicable as between a Member State of the EU, such as Cyprus and a non-EU Member State. However, that Convention does not contain specifically dedicated to cybercrime investigations in general or investigations of online CSE cases in particular either.

Finally, a multilateral agreement, namely the Cybercrime Convention of the Council of Europe acceded by several non-EU countries too and ratified by Cyprus through Law 22(III)/2004 contains substantive law provisions on cybercrime including crimes relating to child pornography as well as provisions on procedural law. Most importantly, it also contains provisions on international co-operation and mutual assistance between contracting states (Articles 23-35 of the Convention). Said provisions can obviously be regarded as being dedicated to *cybercrime* investigations in general including investigations of *online CSE cases* in particular due to the subject-matter of the Convention being cybercrime including online child pornography. It arises that this is the only agreement, specifically, a multilateral one, which contains such provisions.

2.4.3. Bilateral Agreements in Portugal

The framework of judicial and police cooperation binding on the Portuguese State has as its fundamental matrix European Union Law and International Conventional Law, in the latter context with reference to the Council of Europe and the United Nations.

In this context judiciary mutual assistance with EU Member States has is framework governed by the 2001 European Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, as well as the Directive 2014/41/EE regarding the European Investigation Order in criminal matters that has replaced several of the provisions of the said Convention, transposed by Law 38/2017[183]. Regarding specifically the production and exchange of digital evidence, Portugal as already signed the Budapest Convention and their amending Protocols, transposing the legal framework by Law 109/2009[184].

---

[179] Law 20(III)/2006.
[180] This is UN multilateral agreement ratified by Law 11(III)/2003.
[181] This is UN multilateral agreement ratified by Law 25(III)/2008.
[182] This is UN multilateral agreement ratified by Law 19(III)/2000.
[183] https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=2754A0050&nid=2754&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=

[184] https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis

The full list of Multilateral and Bilateral Judicial Cooperation Agreements can be found on the official website of the Procuradoria Geral de República (Attorney General's Office)[185], the Judicial Authority that is normally designated as the Central Authority in the articles.

Given the historical relations outside the Common European Space, Judicial and Police Cooperation Agreements with culturally closer states are relevant. These limited scope Treaties aim at promoting faster and more efficient mechanisms of judicial cooperation in criminal matters, based on the Principle of Mutual Recognition, made necessary by the special relations and migratory movements facilitated by such relations.

In this field, although not specifically incident to or providing for the production and exchange of digital evidence, we should mention the **Convention on Judicial Assistance in Criminal Matters between the Member States of the Community of Portuguese-Speaking Countries[186], adopted by Resolution of the Parliament 46/2008.** The Convention has already been in force for the Republic of Mozambique, the Democratic Republic of São Tomé and Príncipe and the Federative Republic of Brazil since 01/08/2009, for the Republic of Angola since 01/01/2011, and for the Democratic Republic of Timor-Leste since 01/05/2011. Finally, this Convention has been in force in Portugal since 01/03/2010 and in Cape Verde since 01/09/2018. Within is articles there are specific provisions regarding Transmission of requests for assistance (Article 7) allowing communication solely between Central Authorities or communication directly between competent authorities or between them and Central Authorities or between Central Authorities; Requests for assistance encompassed by the Treaty to be made through the International Criminal Police Organization (Interpol) in cases of urgency; and the Spontaneous exchange of information (Article 8).

Also relevant in this context is the **Agreement on Legal and Judicial Cooperation between the Portuguese Republic and the Macao Special Administrative Region of the People's Republic of China,** signed after the ending of the Portuguese administration of the territory in 17/01/2001, setting the parties to endeavor, within the framework of their respective legal systems, and the principles of equality and reciprocity, to encourage and intensify wide intensify wide-ranging and continuous legal and judicial cooperation.

Given its special geographical location, both on the Europe mainland continent and in the Azores and Madeira archipelagos, Portugal has entered into several specific bilateral agreements aimed at combating drug trafficking.

In the area of digital evidence, it is important to highlight the protocols signed by the Attorney General's Office with the American Industry aimed at simplifying and speeding up requests for evidence in cases where this Industry is favourable.

Within the scope of these protocols, with information on the procedures and legal powers of the Portuguese Judicial Authorities, forms and points of contact have been established for the secure exchange of criminal requests and information of a digital nature.

The procedures are defined through binding instructions to the Prosecution Services in the form of the so-called Practice Notes of the Cybercrime Office of the Attorney General's Office.

Specifically on this cooperation subject is the Practice Note No. 3, with detailed information on the cases in which this protocoled way is feasible and the contact points established[187].

---

[185] https://dgpj.justica.gov.pt/Relacoes- Internacionais/Relacoes-bilaterais/Instrumentos-de-cooperacao-judiciaria-internacional

[186] https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1564&tabela=leis

[187] https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_3_isp_eua.pdf

2.4.4. Bilateral Agreements in Germany

Mutual assistance in criminal matters between Germany and foreign states is governed by the International Mutual Assistance Act[188] (IMA Act). In the context of proceedings in a criminal matter relating to a Member State of the EU[189] as well as such proceedings relating to extradition and transit matters involving the Republic of Iceland or the Kingdom of Norway[190], the mutual assistance is governed by the IMA Act. Regarding mutual assistance with other countries, the IMA Act merely provides the default rules because individual bilateral agreements under international law take precedence over the provisions of the IMA Act, as soon and insofar as they have become directly applicable domestic law.[191]

Under the IMA Act[192], it is for the *Federal Ministry of Justice* (in consultation with the Federal Foreign Office and other relevant federal ministries) to give a decision on foreign requests for mutual assistance and to send requests for mutual assistance to foreign states. Although the Federal Government may delegate the exercise of this power to the *Land* governments,[193] this competence has only been transferred to the *Land* governments of the 16 German states for granting incoming and outgoing requests in all matters of the IMA Act with an EU Member State.[194]

As far as non-EU states are concerned, The *Federal Office of Justice* (FOJ) is responsible for deciding on the approval of incoming and outgoing criminal law requests for extradition, enforcement assistance or other legal assistance. In addition, the FOJ is involved in worldwide cooperation in individual cases of criminal legal assistance whenever diplomatic channels or channels to foreign ministries of justice are used (operative competence).

In order to ensure the uniform application of the IMA Act throughout Germany, the Federal Government agreed with all 16 *Land* government on uniform Guidelines for Mutual Assistance with Foreign Countries in Criminal Matters (MACM Guidelines).[195] These MACM Guidelines contain country-specific information on, among other things, the applicable legal basis, the business procedure, the competent authorities abroad, the language regime and special formal requirements. Furthermore, the country section contains references to electronic forms and information material provided by foreign states. For the convenience of courts, public prosecutors and other authorities including LEAs, the FOJ maintains and services the country section of the

[188] Act on International Mutual Assistance in Criminal Matters ("Gesetz über die internationale Rechtshilfe in Strafsachen – IRG").
[189] Section 1(4) IMA Act.
[190] Section 1(5) IMA Act.
[191] Section 1(3) IMA Act.
[192] Section 74(1) IMA Act.
[193] Section 74(2) IMA Act.
[194] Agreement between the Federal Government and the *Land* Governments of Baden-Württemberg, Bavaria, Berlin, Brandenburg, Bremen, Hamburg, Hesse, Mecklenburg-Western Pomerania, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, Saarland, Saxony, Saxony-Anhalt, Schleswig-Holstein and Thuringia on Jurisdiction in Mutual Legal Assistance with Foreign Countries in Criminal Matters („Zuständigkeitsvereinbarung"), 4 May 2004, available at: https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_28042004_935021713162004.htm.
[195] MACM Guidelines („Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten – RiVASt") in version of 23 December 2016, available only in German at: https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_23122016_IIB6935088.htm.

MACM Guidelines in the form a public register[196] providing for each foreign state detailed and up-to-date information on the rules and regulations governing international assistance between Germany and that foreign state.

2.4.4.1. Courtesy Instead of Bilateral Agreement

Germany has no bilateral agreement in place governing international assistance in criminal matters with the following non-EU states: the **Republic of the Phillipines**[197], the **Republic of India**[198], the **People's Republic of China**[199], **Iraq**[200], the **Islamic Republic of Iran**[201], **Argentinia**[202] and **Brasil**[203].

Therefore, mutual assistance between Germany and each of these foreign states is only available via the diplomatic channel based on courtesy and **reciprocity**.

2.4.4.2. Mutual Assistance with USA

There are four bilateral agreements in place governing the mutual assistance in criminal police investigations between Germany and the USA (in chronological order): (i) a bilateral agreement on trafficking illegal drugs;[204] (ii) a bilateral agreement on the disclosure of entries in the criminal register;[205] (iii) a bilateral agreement in addition to the EU's bilateral agreement with the USA on mutual assistance in criminal matters;[206] and (iv) a

[196] The public register of MACM Guidelines is available only in German at: https://www.bmj.de/SiteGlobals/Forms/Suche/RiVaStsuche_Formular.html.
[197] MACM Guidelines on Phillipines („RiVaSt Phillipinen"), April 2018, available in German at: https://www.bmj.de/SharedDocs/Downloads/DE/Service/RiVaSt/Philippinen.pdf.
[198] MACM Guidelines on India („RiVaSt Indien"), June 2020, at section III., available in German at: https://www.bmj.de/SharedDocs/Downloads/DE/Service/RiVaSt/Indien.pdf.
[199] MACM Guidelines on China („RiVaSt China"), April 2018, available in German at: https://www.bmj.de/SharedDocs/Downloads/DE/Service/RiVaSt/China.pdf.
[200] MACM Guidelines on Iraq („RiVaSt Irak"), April 2018, available in German at: https://www.bmj.de/SharedDocs/Downloads/DE/Service/RiVaSt/Irak.pdf.
[201] MACM Guidelines on Iran („RiVaSt Iran"), April 2018, available in German at: https://www.bmj.de/SharedDocs/Downloads/DE/Service/RiVaSt/Iran.pdf.
[202] MACM Guidelines on Argentina („RiVaSt Argentinien"), April 2022, available in German at: https://www.bmj.de/SharedDocs/Downloads/DE/Service/RiVaSt/Argentinien.pdf.
[203] MACM Guidelines on Brasil („RiVaSt Brasilien"), March2012, available in German at: https://www.bmj.de/SharedDocs/Downloads/DE/Service/RiVaSt/Brasilien.pdf.
[204] Notenwechsel vom 17. Januar / 24. August 1955 / 7. März 1956 über die Bekämpfung des ungesetzlichen Verkehrs mit Betäubungsmitteln, BGBl. 1957 II S. 709.
[205] Notenwechsel vom 7. November / 28. Dezember 1960 /3. Januar 1961 über den Rechtshilfeverkehr in Strafsachen und über die Erteilung von Auskünften aus dem Strafregister, BGBl. 1961 II S. 471.
[206] Vertrag vom 14. Oktober 2003 zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe i.V.m. dem Zusatzvertrag vom 18. April 2006 zum Vertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen, BGBl. 2007 II S. 1617.

bilateral agreement on mutual assistance in preventing and fighting serious crime.[207]

Out of these four bilateral agreements, only the bilateral agreement (iv) concerning serious crime contains provisions governing the processing of personal data of suspected individuals. However, the bilateral agreement (iv) offers mutual access to fingerprint data[208] as well as automated searches of DNA profiles[209]. Therefore, the bilateral agreement (iv) seems unlikely to be of immediate relevance in cybercrime investigations. Rather, this bilateral agreement (iv) appears to extend the framework provided by the EU *Prüm* decisions for Germany to the USA.

Nevertheless, German LEAs may request **mutual assistance in criminal investigations** insofar as: (1) information is to be obtained, (2) police documents or files are to be obtained, (3) the whereabouts of persons are to be determined or (4) persons are to be questioned by the police.[210]

2.4.4.3. Mutual Assistance with Russia

In general, mutual assistance between Germany and the Russian Federation is governed by the European Convention on Mutual Assistance in Criminal Matters[211] and its First[212] and Second[213] Additional Protocol. In addition, mutual assistance in criminal police investigations between Germany and the Russian Federation is governed by a bilateral agreement on cooperation on combating crimes of significance.[214]

None of these bilateral agreements between Germany and the Russian Federation contains provisions specifically dedicated to *cybercrime* investigations in general or investigations of *online CSE cases* in particular.

2.4.5. Bilateral Agreements in Lithuania

Lithuania has signed and ratified bilateral agreements on cooperation on fight against crime with eight non EU

---

[207] Abkommen vom 1. Oktober 2008 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität, BGBl. 2009 II S. 1010. This bilateral agreement is available in English at German Bundestag, Ds. 16/13123, pp. 7-14, see: https://dserver.bundestag.de/btd/16/131/1613123.pdf

[208] Art. 3 and 4 of the bilateral agreement (iv), see previous footnote.

[209] Art. 7 of the bilateral agreement (iv), see previous footnote.

[210] MACM Guidelines on USA („RiVaSt Vereinigte Staaten"), 21 October 2009, section III.2. (last paragraph), available in German at: https://www.bmj.de/SharedDocs/Downloads/DE/Service/RiVaSt/Vereinigte_Staaten.html.

[211] CoE, European Convention on Mutual Assistance in Criminal Matters, 20 April 1959, ETS No. 030, available at: https://rm.coe.int/16800656ce.

[212] CoE, Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, 17 March 1978, ETS No. 099, available at: https://rm.coe.int/1680077975.

[213] CoE, Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, 8 November 2001, ETS No. 182, available at: https://rm.coe.int/168008155e.

[214] Abkommen vom 3. Mai 1999 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Russischen Föderation über Zusammenarbeit bei der Bekämpfung von Straftaten von erheblicher Bedeutung, BGBl. 2004 II S. 860; 2005 II S. 621.

countries: **Israel**[215], **Georgia**[216], **Serbia**[217], **USA**[218], **Ukraine**[219], **Kazakhstan**[220], **Belorussia**[221] and **Turkey**[222]**.** Cyber crime and partly CSEM as separate domain is specified only in agreement with **Israel.** Agreements with **Georgia** and **Serbia** lists cybercrime or child sexual exploration crimes as areas of cooperation but does not contain any special provisions or requirements.

2.4.5.1. Mutual Assistance with Israel

Mutual assistance in criminal matters between Lithuania and Israel is based on Agreement of The Government of the Republic of Lithuania and the Government of the State of Israel on Cooperation on Public Security and Fight Against Crime[223]. The areas of cooperation are:

1. law enforcement to fight against organized crime, terrorism and terrorism financing, trafficking in persons, illegal migration, **cybercrime**, money laundering and financial crimes, corruption crimes, illicit trafficking of narcotic drugs, psychotropic substances and precursors, illicit production, trafficking and disposal of firearms and explosive materials, forgery of documents and distribution thereof, and other crimes;
2. public security in public events/ mass gatherings;

---

[215] Lietuvos Respublikos Vyriausybės ir Izraelio Valstybės Vyriausybės susitarimas dėl bendradarbiavimo viešojo saugumo ir kovos su nusikalstamumu srityse, https://www.e-tar.lt/portal/lt/legalAct/bff942e07af911e9863cb9ed35b4647a

[216] Lietuvos Respublikos Vyriausybės ir Gruzijos Vyriausybės susitarimas dėl bendradarbiavimo kovojant su nusikalstamumu, https://www.e-tar.lt/portal/lt/legalAct/41e31e40b03b11e48296d11f563abfb0

[217] Lietuvos Respublikos Vyriausybės ir Serbijos Respublikos Vyriausybės susitarimas dėl bendradarbiavimo kovojant su nusikalstamumu, https://www.e-tar.lt/portal/lt/legalAct/31d5ab70d2cf11e8bea9885f77677ec1

[218] Lietuvos Respublikos Vyriausybės ir Jungtinių Amerikos Valstijų Vyriausybės susitarimas dėl glaudesnio bendradarbiavimo nusikaltimų prevencijos ir kovos su jais srityje, https://www.e-tar.lt/portal/lt/legalAct/TAR.3FC4F4FDB53B

[219] Lietuvos Respublikos Vyriausybės ir Ukrainos Ministrų Kabineto susitarimas dėl bendradarbiavimo kovojant su nusikalstamumu ir tarptautiniu terorizmu, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.314721

[220] Lietuvos Respublikos Vyriausybės ir Kazachstano Respublikos Vyriausybės susitarimas dėl bendradarbiavimo kovojant su organizuotu nusikalstamumu, neteisėta narkotinių ir psichotropinių medžiagų apyvarta, terorizmu ir kitais nusikaltimais, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.132158

[221] Lietuvos Respublikos Vyriausybės ir Baltarusijos Respublikos Vyriausybės susitarimas dėl bendradarbiavimo kovojant su organizuotu nusikalstamumu, neteisėta narkotinių ir psichotropinių medžiagų ir jų pirmtakų apyvarta, terorizmu ir kitais nusikaltimais, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.303570

[222] Lietuvos Respublikos Vyriausybės ir Turkijos Respublikos Vyriausybės susitarimas dėl bendradarbiavimo kovojant su terorizmu, organizuotu nusikalstamumu, neteisėta narkotinių priemonių ir psichotropinių medžiagų apyvarta (prekyba jomis) ir kitais sunkiais nusikaltimais, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.238876

[223] Lietuvos Respublikos Vyriausybės ir Izraelio Valstybės Vyriausybės susitarimas dėl bendradarbiavimo viešojo saugumo ir kovos su nusikalstamumu srityse, https://www.e-tar.lt/portal/lt/legalAct/bff942e07af911e9863cb9ed35b4647a

3. crime and delinquency prevention;
4. investigation and intelligence for public security;
5. witness protection.

The mutual cooperation in cybercrime is regulated by Art. 5 of this agreement. It requires Lithuania and Israel to designate a point of contact available on a twenty-four hour, seven-day-a-week basis according to the Budapest Convention in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence (including in real time, where appropriate/feasible) regarding the following matters:

1. the commission of an offence using computer networks or electronic information;
2. the preservation and production of data in cases where there are grounds to believe that the data will otherwise disappear;
3. threats to public order and/or national security of the requesting country.

Additionally, each of the country ensures that trained and equipped personnel are available in order to facilitate the handling of above mentioned requests and **collaborate in identifying natural or legal persons involved in the production, distribution, procurement or possession of child pornography.**

2.4.5.2. Mutual Assistance with Georgia

Mutual assistance in criminal matters between Lithuania and Georgia is based on Agreement of The Government of the Republic of Lithuania and the Government of Georgia on Cooperation in the Fight Against Crime[224]. The areas of cooperation include cybercrime[225]. However, there are no special provisions in the agreement related to CSEM, cybercrime investigation or electronic surveillance.

2.4.5.3. Mutual Assistance with Serbia

Mutual assistance in criminal matters between Lithuania and Serbia is based on Agreement of the Government of the Republic of Lithuania and the Government of the Republic of Serbia on Cooperation in Combating Crime[226]. The areas of cooperation include child sexual exploration crimes in general[227]. There are no special provisions on CSEM, cybercrime investigation or electronic surveillance.

[224] Lietuvos Respublikos Vyriausybės ir Gruzijos Vyriausybės susitarimas dėl bendradarbiavimo kovojant su nusikalstamumu, https://www.e-tar.lt/portal/lt/legalAct/41e31e40b03b11e48296d11f563abfb0

[225] Art. 2 of the Agreement.

[226] Lietuvos Respublikos Vyriausybės ir Serbijos Respublikos Vyriausybės susitarimas dėl bendradarbiavimo kovojant su nusikalstamumu, https://www.e-tar.lt/portal/lt/legalAct/31d5ab70d2cf11e8bea9885f77677ec1

[227] Art. 2 of the Agreement.

3. Criminalisation of CSEM

CSEM is one of the most regulated areas of illegal content with broad international consensus that the harm of such material is so substantial, that it requires extensive criminalisation. The following chapter provides a brief overview of the international standards built on this global consensus as background information for all researchers participating in the GRACE project on the reasons why there are highly complex processes in place preventing any researcher from access to CSEM. From a developer's perspective, the processes highly complicate the development of the GRACE solution as an immediate feedback is missing. However, it is the nature of the international legal standards that anybody accessing CSEM faces criminal liability apart only from authorized LEAs. Based on the intended purpose of this chapter, the decision was taken that the extent of criminalisation does not need to be canvassed in the country reports (chapters 10.–14. below).

3.1. International Standards

While the UN Convention on the Rights of the Child[228] does not explicitly mention CSEM or child pornography,[229] the 2000 Optional Protocol to the Convention does already address the issue in the title.[230] Three articles are of particular relevance: Art. 2, Art. 3 and Art. 10:

> ***Article 2***
>
> *For the purposes of the present Protocol:*
>
> *(a) Sale of children means any act or transaction whereby a child is transferred by any person or group of persons to another for remuneration or any other consideration;*
>
> *(b) Child prostitution means the use of a child in sexual activities for remuneration or any other form of consideration;*
>
> *(c) Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.*

> ***Article 3***
>
> *1. Each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether such offences are committed domestically or transnationally or on an individual or organized basis:*
>
> *(a) In the context of sale of children as defined in article 2:*
>
> *(i) Offering, delivering or accepting, by whatever means, a child for the purpose of:*

[228] United Nations Convention on the Rights of the Child, 1989.
[229] This Deliverable D9.3 predominantly refers to CSEM which covers not only child sexual exploitation but also child sexual abuse material, both of which are referred to in legislation as "child pornography". For more information on the impact of terminology see section 3 of Deliverable D10.6.
[230] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 2000. Regarding the child pornography related content of the Optional Protocol see: *Gercke*, Understanding Cybercrime, ITU, 2014, Chapter 6.2.8.

a. Sexual exploitation of the child;

b. Transfer of organs of the child for profit;

c. Engagement of the child in forced labour;

(ii) Improperly inducing consent, as an intermediary, for the adoption of a child in violation of applicable international legal instruments on adoption;

(b) Offering, obtaining, procuring or providing a child for child prostitution, as defined in article 2;

(c) Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography as defined in article 2.

2. Subject to the provisions of the national law of a State Party, the same shall apply to an attempt to commit any of the said acts and to complicity or participation in any of the said acts.

3. Each State Party shall make such offences punishable by appropriate penalties that take into account their grave nature.

4. Subject to the provisions of its national law, each State Party shall take measures, where appropriate, to establish the liability of legal persons for offences established in paragraph 1 of the present article. Subject to the legal principles of the State Party, such liability of legal persons may be criminal, civil or administrative.

5. States Parties shall take all appropriate legal and administrative measures to ensure that all persons involved in the adoption of a child act in conformity with applicable international legal instruments.

Article 10

1. States Parties shall take all necessary steps to strengthen international cooperation by multilateral, regional and bilateral arrangements for the prevention, detection, investigation, prosecution and punishment of those responsible for acts involving the sale of children, child prostitution, child pornography and child sex tourism. States Parties shall also promote international cooperation and coordination between their authorities, national and international non-governmental organizations and international organizations.

2. States Parties shall promote international cooperation to assist child victims in their physical and psychological recovery, social reintegration and repatriation.

3. States Parties shall promote the strengthening of international cooperation in order to address the root causes, such as poverty and underdevelopment, contributing to the vulnerability of children to the sale of children, child prostitution, child pornography and child sex tourism.

4. States Parties in a position to do so shall provide financial, technical or other assistance through existing multilateral, regional, bilateral or other programmes.

The definition of “child pornography” in Art.2 c) and the description the conduct that should be criminalized in Art. 3 (1) c) of the Optional Protocol can today be considered standard when it comes to criminalizing CSEM. Art. 3 clarifies that the criminalization should not be limited to the production or distribution of such material but should include any possession “child pornography”. However, Art. 3 does not include language that specifically addresses issues like “online streaming” of CSEM. In 2019 the United Nations followed up by

publishing Guidelines that support Member States in implementing the Optional Protocol.[231]

3.2. Council of Europe

3.2.1. Convention on Cybercrime

20 years after opening for signature, the Council of Europe Convention on Cybercrime[232] remains an important regional source when it comes to the criminalization of Cybercrime. In order to improve and harmonize the protection of children against sexual exploitation,[233] the Convention on Cybercrime includes an article addressing "child pornography". Taking into account that most Council of Europe Member States had already criminalized the abuse of children as well as traditional methods of distribution of "child pornography" by the time the Convention was opened for signature,[234] the aim of the Art. 9 is thus not limited to closing gaps in national criminal law[235] – this provision also seeks to harmonize differing regulation.[236]

> ***Article 9 – Offences related to child pornography***
>
> *(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:*

---

[231] Guidelines regarding the implementation of the Optional Protocol on the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 2019, CRC/C156.

[232] Council of Europe Convention on Cybercrime, ETS 185. See in this regard: CETS 185: Council of Europe Convention on Cybercrime. For more information see: *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225,; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, CRi 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, CRi 2008, page 7 *et seq.*; *Gercke*, 10 years Convention on Cybercrime, Cri 2011, 142 *et seq*.; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

[233] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

[234] *Akdeniz* in *Edwards/Waelde*, Law and the Internet: Regulating Cyberspace; *Williams* in *Miller*, Encyclopaedia of Criminology, page 7. Regarding the extent of criminalization, see: Child Pornography: Model Legislation & Global Review, 2006, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalization of child pornography and freedom of speech in the United States, see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws in terms of the criminalization of child pornography.

[235] Regarding differences in legislation, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 26, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[236] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

a) producing child pornography for the purpose of its distribution through a computer system;

b) offering or making available child pornography through a computer system;

c) distributing or transmitting child pornography through a computer system;

d) procuring child pornography through a computer system for oneself or for another person;

e) possessing child pornography in a computer system or on a computer-data storage medium.

(2) For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct;

b) a person appearing to be a minor engaged in sexually explicit conduct;

c) realistic images representing a minor engaged in sexually explicit conduct.

(3) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

(4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

The criminalization described in Art. 9 of the CoE Convention on Cybercrime is largely in line with the standards described in the 2000 Optional Protocol to the UN Convention on the Rights of the Child.[237] Just like the Optional Protocol at UN level, the CoE Convention on Cybercrime does not specifically address more recent way CSEM is consumed – such as streaming video.

3.2.2. Convention on the Protection of Children

In 2007 the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CoE Convention on the Protection of Children) was opened for signature.[238] Unlike the 2001 Convention on Cybercrime, it does not specifically focus on online crimes but addresses the need for criminalization of both traditional as well as online offences.

Article 20 – Offences concerning child pornography

(1) Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:

a) producing child pornography;

b) offering or making available child pornography;

c) distributing or transmitting child pornography;

[237] For details see: *Gercke*, Understanding Cybercrime, ITU, 2014, Chapter 6.2.8.
[238] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

d) procuring child pornography for oneself or for another person;

e) possessing child pornography;

f) knowingly obtaining access, through information and communication technologies, to child pornography.

(2) For the purpose of the present article, the term "child pornography" shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes.

(3) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:

– consisting exclusively of simulated representations or realistic images of a non-existent child;

– involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.

(4) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f

Art. 20 (1) (a)–(f) is largely in line with the UN Optional Protocol to the Convention on the Rights of the Child and the CoE Convention on Cybercrime Art. 20 (1) (f) specifically addresses Internet related conduct.

3.3. European Union

The European Union has undertaken several steps to harmonise the legislation related to CSEM among the EU Member States. The most relevant legal framework in this regard to the 2011 EU Directive on Combatting Child Pornography.[239] While Art. 2(c) defines the term "child pornography" for the purposes of this Directive, Art. 5 of this Directive specifically addresses the issue of CSEM.

Article 5 - Offences concerning child pornography

1. Member States shall take the necessary measures to ensure that the intentional conduct, when committed without right, referred to in paragraphs 2 to 6 is punishable.

2. Acquisition or possession of child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.

3. Knowingly obtaining access, by means of information and communication technology, to child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.

4. Distribution, dissemination or transmission of child pornography shall be punishable by a maximum term of imprisonment of at least 2 years.

[239] Directive 2011/93/EU of the European Parliament and the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA. Regarding details see: *Gercke*, EU Directive to fight child pornography, Computer und Recht, 2012, page 520 et seq.

5. Offering, supplying or making available child pornography shall be punishable by a maximum term of imprisonment of at least 2 years.

6. Production of child pornography shall be punishable by a maximum term of imprisonment of at least 3 years.

7. It shall be within the discretion of Member States to decide whether this Article applies to cases involving child pornography as referred to in Article 2(c)(iii), where the person appearing to be a child was in fact 18 years of age or older at the time of depiction.

8. It shall be within the discretion of Member States to decide whether paragraphs 2 and 6 of this Article apply to cases where it is established that pornographic material as referred to in Article 2(c)(iv) is produced and possessed by the producer solely for his or her private use in so far as no pornographic material as referred to in Article 2(c)(i), (ii) or (iii) has been used for the purpose of its production and provided that the act involves no risk of dissemination of the material.

Art. 5 is in line with international best practices, especially Art. 20 CoE Convention on the Protection of Children. Just like the CoE Convention it does specifically address Internet-related conduct.

3.4. Conclusion for GRACE

Task T9.2 has two main focuses: Analysing the legal environment LEAs will be operating the GRACE solution in and highlighting areas that researchers involved in the development need to be mindful about while performing their work.

With regard to both – LEAs and researchers – it is important to underline that the applicable international and regional frameworks do not include any specific exemption from criminal liability for individual LEA officers or researchers. As a consequence, both LEA officers and researchers have to be mindful about the fact that they face possible criminal sanctions when interacting with CSEM unless national law provides an exemption for their respective activity. As within the work carried out under Task 9.2 no exemptions for research purposes in general and individual researchers in particular could be identified, all researchers and other non-LEA experts involved in the GRACE project should avoid any direct interaction with CSEM. LEAs should solely act within the exemptions provided for them by national law.

4. EU-Proposal for Harmonised Framework Against Online CSA

This chapter takes a closer look at the regulatory framework on preventing and combating online child sexual abuse (CSA) proposed by the European Commission in May 2022 and provides a first analysis how this future regulatory framework may affect to the tools and platform developed in the course of the GRACE project.

On 11 May 2022, the Commission introduced the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse[240] (Draft Regulation Against Online CSA) in the EU's legislative process. The proposed Draft Regulation Against Online CSA reflects the priority given to the protection of children, both offline and online, within the EU and emanating from Art. 24(2) EU-Charter of Fundamental Rights as well as from the United Nations Convention on the Rights of the Child (CRC).[241] After two Reports on the implementation of the 2011 EU Directive on Combatting Child Pornography[242] had revealed significant shortcomings in protecting children from falling victim to CSA in 2016, the 2020 EU Strategy for a More Effective Fight Against CSA[243] and the 2021 EU Strategy on the Rights of the Child[244] paved the way for the Draft Regulation Against Online CSA which may serve as evidence for the commitment expressed in the European Declaration on Digital Rights and Principles[245] to protect all children against harmful and illegal content, exploitation, manipulation and abuse online, and preventing the digital space from being used to commit or facilitate crimes.

A global survey conducted by Economist Impact in 2021 had found that half of respondents had experienced a form of CSA online during their childhood, while more than a third had been asked to do something sexually

[240] Commission, Proposal for a Regulation of the European Parliament and the Council laying down rules to prevent and combat child sexual abuse, COM (2021) 209 final, 2022/0155 (COD), 11 May 2022, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209&from=EN.

[241] Commission, Draft Regulation Against Online CSA, COM (2021) 209 final, 11 May 2022, Explanatory Memorandum, p. 1. For more details on the United Nations Convention on the Rights of the Child see section 6.1 below.

[242] Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, COM/2016/0871 final, 16 December 2016, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0871; and Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, COM/2016/0872 final, 16 December 2016, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2016:872:FIN.

[243] Commission, „EU strategy for a more effective fight against child sexual abuse", Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020) 607 final, 24 July 2020; available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0607.

[244] Commission, „EU strategy on the rights of the child", Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2021) 142 final, 24 March 2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0142.

[245] European Parliament/Council/Commission, „European Declaration on Digital Rights and Principles fort he Digital Decade", signed on 15 December 2022, committment in Chapter V. lit. (c) after No. 22., available at: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

explicit online.[246] Against this background, the WeProtect Alliance of more than 200 governments, private sector companies and civil society organisations included as policy recommendation that laws should establish standards for industry reporting, the rapid removal of child sexual abuse material, and a basis for the lawful and transparent use of tools to detect child sexual abuse material and pointed out the effects of placing legal responsibilities on online service providers.[247]

First, the objectives and the approach of the Draft Regulation Against Online CSA are presented (section 4.1 below). Second, it is examined how the Draft Regulation Against Online CSA affects the GRACE tools and platform (section 4.2. below).

4.1. Objectives & Approach of the Regulation Against Online CSA

Recognising that the responsible and diligent behaviour of providers of hosting or interpersonal communication services (providers) is essential for a safe, predictable and trusted online environment,[248] the Draft Regulation Against Online CSA aims to shift the balance between the societal interest in preventing and combating CSA online to protect the fundamental rights of child victims[249], on the one side, and the fundamental rights of users[250] and of the providers[251], on the other, in favour of the (potential) child victims.[252] For this purpose, the Draft Regulation Against Online CSA consists of two main building blocks.

[246] WeProtect Global Alliance, „Estimates of Childhood Exposure to Online Sexual Harms and Their Risk Factors: A Global Study of Childhood Experiences of 18 to 20 Year Olds“, 2021, conducted by Economist Impact with more than 5,000 respondents in 54 countries and available at: https://www.weprotect.org/economist-impact-global-survey/#report.

[247] WeProtect Global Alliance, „Global Threat Assessment 2021“, p. 7 and p. 64; available at: https://www.weprotect.org/global-threat-assessment-21/#report.

[248] Commission, Draft Regulation Against Online CSA, COM (2021) 209 final, 11 May 2022, Explanatory Memorandum, p. 2.

[249] Weighed are the *children's* fundamental rights to human dignity (Art. 1 EU-Charter of Fundamental Rights), to integrity of the person (Art. 3 EU-Charter of Fundamental Rights), to respect for private and family life (Art. 7 EU-Charter of Fundamental Rights) and to protection of personal data (Art. 8 EU-Charter of Fundamental Rights) as well as the prohibition of degrading treatment (Art. 4 EU-Charter of Fundamental Rights) and the rights of the child (Art. 24 EU-Charter of Fundamental Rights). Commission, Draft Regulation Against Online CSA, COM (2021) 209 final, 11 May 2022, Explanatory Memorandum, p. 12.

[250] Weighed are the *users'* fundamental rights to respect for privacy (as part of the right to respect for private and family life, Art. 7 EU-Charter of Fundamental Rights), to protection of personal data (Art. 8 EU-Charter of Fundamental Rights) and to freedom of expression (Art. 11 EU-Charter of Fundamental Rights). Commission, Draft Regulation Against Online CSA, COM (2021) 209 final, 11 May 2022, Explanatory Memorandum, p. 12 et seq.

[251] Weighed is the *providers'* fundamental freedom to conduct a business (Art. 16 EU-Charter of Fundamental Rights). Commission, Draft Regulation Against Online CSA, COM (2021) 209 final, 11 May 2022, Explanatory Memorandum, p. 13.

[252] Commission, Draft Regulation Against Online CSA, COM (2021) 209 final, 11 May 2022, Explanatory Memorandum, pp. 12 to 15.

4.1.1. Scope

Based on the legislative competence to establish measures to ensure the functioning of the Internal Market,[253] the Draft Regulation Against Online CSA aims to harmonise the rules applicable on the detection, reporting and removal of online CSA as necessary measure to remove existing national barriers to the Digital Single Market and to complement the Digital Services Act.[254] To achieve this objective, the Draft Regulation Against Online CSA introduces targeted and uniform obligations of risk assessment[255] and mitigation[256] which are complemented where necessary by orders for detection[257], reporting[258] and removal[259] of CSA content. These obligations are applicable to any provider offering hosting or interpersonal communication services on the Digital Single Market regardless of where they have their principal establishment.[260]

The application and enforcement of these obligations in particular and the Draft Regulation Against Online CSA in general is placed under the responsibility of independent[261] national Coordinating Authorities designated by the Member States for the consistent application, Art. 25(2) Draft Regulation Against Online CSA. For this purpose, the Coordinating Authorities are granted investigatory powers in respect of providers enabling them to:[262] (a) require providers to provide information; (b) carry out on-site inspections of any providers' premises for information on suspected infringements; (c) ask any of a provider's staff for explanations about suspected infringements; and (d) assess a provider's compliance with a detection, removal or blocking order. Most interesting in the context of the GRACE project, the Coordinating Authorities' investigatory powers also include the power to monitor compliance with the Draft Regulation Against Online CSA by conducting searches on publicly accessible material to detect known or new CSA material,[263] as well as the power to notify a provider of known CSA material on their services and to request the provider to voluntarily remove or disable access to it.[264]

Furthermore, the Coordinating Authorities are also granted enforcement powers to ensure a provider's compliance with the requirements of the Draft Regulation Against Online CSA ranging from accepting[265] a

[253] Art. 114 TFEU, see: Commission, Draft Regulation Against Online CSA, COM (2021) 209 final, 11 May 2022, Explanatory Memorandum, p. 4.
[254] Art. 1(3)(b) and Art. 2(a), (g), (r), (t) and (v) as well as Rec. (15), (16), (31), (40) and (42) Draft Regulation Against Online CSA. Commission, Draft Regulation Against Online CSA, COM (2021) 209 final, 11 May 2022, Explanatory Memorandum, p. 2.
[255] Art. 3 Draft Regulation Against Online CSA.
[256] Art. 4 Draft Regulation Against Online CSA.
[257] Art. 7 and 8 Draft Regulation Against Online CSA.
[258] Art. 5 Draft Regulation Against Online CSA.
[259] Art. 1(c) and (d) Draft Regulation Against Online CSA alluding to the removal order against an ISP under Art. 14 Draft Regulation Against Online CSA and to the blocking order against an access provider under Art. 16 Draft Regulation Against Online CSA, depending on whether ISPs offer their services in the EU, Re. (32) Draft Regulation Against Online CSA.
[260] Art. 1(2) and Rec. (6) Draft Regulation Against Online CSA.
[261] According to Art. 26(2) Draft Regulation Against Online CSA, the Member States shall ensure that the Coordinating Authorities: (a) are legally and functionally independent from any other public authority; (b) have status to carry out their tasks objectively and impartially; (c) are free from any external influence; (d) neither seek nor take instructions from anyone; and (e) are solely charged with their tasks under the Draft Regulation Against Online CSA.
[262] Art. 27(1) Draft Regulation Against Online CSA.
[263] Art. 31 Draft Regulation Against Online CSA.
[264] Art. 32 Draft Regulation Against Online CSA.
[265] Art. 28(1)(a) Draft Regulation Against Online CSA.

provider's commitment over imposing[266] remedies, fines or periodic penalty payments up to ordering[267] the temporary restriction of user access to the service.

In the interest of proportionality, these harmonised obligations only apply to providers of those types of online services which have proven to be vulnerable to misuse for the purpose of dissemination of either CSA content or solicitation of children[268] because of their technical features or the age composition of their typical user base.[269] However, imposing obligations concerning the detection, reporting, removal and blocking of known and new CSA material as well as solicitation of children[270] constitutes only the first building block of the Draft Regulation Against Online CSA.

4.1.2. EU Centre on CSA

Most interesting for the development and potential future dissemination of the GRACE tools and platform is the second building block which establishes the EU Centre on CSA (EU Centre) as a new EU Agency to prevent and combat CSA.[271] This EU Centre is intended to perform various tasks into which the research and development performed in the course of the GRACE project appears to feed into. The tasks of the EU Centre include the assessment of a provider's report on CSA (section 4.1.2.1 below), the operation of databases for CSA reports and indicators (section 4.1.2.2 below) and the making available of detection technologies (section 4.1.2.3 below).

4.1.2.1. Reports on CSA

The regulated providers have to report immediately any instance of potential online CSA to the EU Centre.[272] For these reports, Annex III of the Draft Regulation Against Online CSA provides a mandatory template in which the reporting provider has to provide the equally mandatory information detailed in Art. 13(1) sentence 2 (a)-(k) Draft Regulation Against Online CSA:

(a) identification details of the provider and, where applicable, its legal representative;

(b) the date, time stamp and electronic signature of the provider;

(c) all content data, including images, videos and text;

(d) all available data other than content data related to the potential online CSA;

(e) whether the potential online child sexual abuse concerns the dissemination of known or new CSA

[266] Art. 28(1)(b)-(e) Draft Regulation Against Online CSA.
[267] Art. 29(2)(b) Draft Regulation Against Online CSA.
[268] Known as „grooming".
[269] These obligations are imposed on the providers regardless of the technology used in the online exchanges, Rec. (5) Draft Regulation Against Online CSA, and leave the choice of the technologies operated for compliance with the requirements and measures up to the provider concerned, Rec. (24) Draft Regulation Against CSA.
[270] These obligations are imposed on the providers regardless of the technology used.
[271] Art. 40 Draft Regulation Against Online CSA.
[272] Art. 12(1) Draft Regulation Against Online CSA.

material or the solicitation of children;

(f) information concerning the geographic location related to the potential online CSA, such as the Internet Protocol address;

(g) information concerning the identity of any user involved in the potential online CSA;

(h) whether the provider has also reported, or will also report, the potential online CSA to a public authority or other entity competent to receive such reports of a third country and if so, which authority or entity;

(i) where the potential online CSA concerns the dissemination of known or new CSA material, whether the provider has removed or disabled access to the material;

(j) whether the provider considers that the report requires urgent action;

(k) a reference to this Regulation as the legal basis for reporting.

This detailed list of mandatory information for reports on potential CSA seems remarkably similar to the information provided in the CSEM reports referred to Europe by the US-American NCMEC and the Canadian NCECC. However, the reports pursuant to Art. 12(1) in conjunction with Art. 13(1) and Annex III Draft Regulation Against Online CSA are not submitted directly to Europol or national LEAs. Rather, these European CSA reports are shared at first solely with the EU Centre via a secure information sharing system.[273]

Having received such a report, the EU Centre has to assess whether the report is "manifestly unfounded" in order to avoid obvious false positives.[274] When the EU Centre considers a report to be "manifestly unfounded", the EU Centre has to inform the reporting provider to that extent and specify the reasons.[275] In case the EU Centre considers a report "not manifestly unfounded", the EU Centre has to forward the report to Europol and to the competent national LEA(s) likely to have jurisdiction to investigate and prosecute the potential CSA of the report.[276] As a result, the EU Centre acts as reporting centre and clearing house for reports on CSA in Europe. This function of the EU Centre appears equivalent to the role of the NCMEC in the USA and the role of the NCECC in Canada and, ultimately, increases the number of CSEM reports referred to law enforcement in the EU by the number of CSA reports.

4.1.2.2. Databases for CSA Reports and Indicators

Not surprisingly, the EU Centre is mandated to operate a database for all the CSA reports submitted to it by providers, Art. 45(1) Draft Regulation Against CSA. This database is intended to contain not only each individual CSA report[277], but also detailed information about the EU Centre's assessment and the exact

[273] The EU Centre has to establish and maintain a reliable and secure information sharing system for communications between the providers of regulated services and the EU Centre, Art. 39(2) Draft Regulation Against Online CSA, and this information sharing system has to be used for the reports, Art. 12(1) sentence 2 Draft Regulation Against Online CSA.
[274] Art. 43(3)(b) in conjunction with Art. 48(1) Draft Regulation Against Online CSA.
[275] Art. 48(2) Draft Regulation Against Online CSA.
[276] Art. 48(3) Draft Regulation Against Online CSA.
[277] Art. 45(2)(a) Draft Regulation Against Online CSA.

further handling of each CSA report[278] as well as the *relevant indicators* and ancillary tags associated with the reported potential CSA material.[279]

In addition, the EU Centre is mandated to create and operate databases of three types of indicators of online CSA, Art. 44(1) Draft Regulation Against Online CSA: (a) indicators to detect known CSA material; (b) indicators to detect unknown CSA material; and (c) indicators to detect the solicitation of children. Each of these databases may solely contain the *relevant indicators* and the necessary additional information facilitating their use[280]. The *relevant indicators* are defined as „digital identifiers to be used to detect the dissemination of known or new CSA material or the solicitation of children"[281] and include also a list of uniform resource locators (URLs) in the database of indicators to detect known CSA material[282].

The EU Centre is expected to generate the *relevant indicators* solely on the basis of CSA material submitted to it by national Coordinating Authorities,[283] while the URLs indicating specific items of CSA material hosted by a provider not offering services in the EU may only be submitted to the EU Centre once the national Coordination Authority has exhausted both alternative options to have the CSA material removed either voluntarily or forcefully via mutual legal assistance.[284]

4.1.2.3. Detection Technologies

The EU Centre is also mandated to make available relevant technologies for the execution of detection orders[285] and to act as information and expertise hub[286] collecting information and supporting research and information sharing in the area of online CSA.

In the context of the GRACE project, it seems highly interesting to note that, having received a detection order, a provider is entitled to acquire, install and operate free of charge the technologies made available by the EU Centre in this respect for detecting known or new CSA material (or the solicitation of children),[287] whereas the EU Centre may otherwise make these technologies available under reasonable licensing conditions.[288] For this purpose, the EU Centre has to compile and maintain lists of such technologies.[289]

[278] Art. 45(2)(b)-(f) Draft Regulation Against Online CSA.
[279] Art. 45(2)(g) Draft Regulation Against Online CSA.
[280] Art. 44(2)(c) Draft Regulation Against Online CSA.
[281] Art. 44(2)(a) Draft Regulation Against Online CSA.
[282] Art. 44(2)(b) Draft Regulation Against Online CSA.
[283] Art. 44(3) subparagraph 1 in conjunction with Art. 36(1)(a) Draft Regulation Against Online CSA.
[284] Art. 44(3) subparagraph 2 in conjunction with Art. 36(1)(b) Draft Regulation Against Online CSA.
[285] Art. 50(1) Draft Regulation Against Online CSA.
[286] Art. 50(2) and (3) Draft Regulation Against Online CSA.
[287] Art. 10(1) and (2) Draft Regulation Against Online CSA.
[288] Art. 50(1) subparagraph 1 Draft Regulation Against Online CSA.
[289] Art. 50(1) subparagraph 2 and 3 Draft Regulation Against Online CSA.

4.2. Effect on GRACE Tools and Platform

The comprehensive mandate of the new EU Centre envisioned in the Draft Regulation Against Online CSA seems to produce rather fertile ground to benefit from the research performed in the course of the GRACE project but also a potential use of the GRACE tools and platform. All three focus areas of the EU Centre's mandate could positively be affected by the prioritisation of CSEM reports (section 4.2.1 below) and concerning CSEM indicators, detection tools and trend analysis (section 4.2.2 below).

4.2.1. Prioritisation of CSEM Reports

For a start, the GRACE tools and platform aim to deliver significant operational value to Europol and national LEAs across Europe in tackling the total volume of international online CSEM reports increased by the European CSA reports (addressed together as CSEM reports). The high-level analytical GRACE tools made available to LEAs via a Federated Platform aim to transform their investigative capabilities into a synchronised and impactful response to the immense influx of CSEM reports. The GRACE project develops Big Data solutions for data ETL[290] which not only standardise the management of CSEM reports, but also avoid duplicate processing and enhance collaboration amongst national LEAs within the EU. The data of each CSEM report is analysed in terms of visual, audio and text information using AI technologies to produce structured and validated information from the CSEM report's content.

For this purpose, GRACE develops novel forensic analysis tools for (i) CSEM-specific content analysis and classification, (ii) content-based geo-localisation, (iii) the creation of evidence graphs to connect cases, (iv) case prioritisation techniques and (v) predictive analysis of trends in CSE offenders' tactics. For the operational coordination of LEAs in all Member States, a Federated (Machine) Learning platform are developed and established which can exploit available infrastructure as well as the metadata of any CSEM content distributed across the entire EU.

4.2.2. CSEM Indicators, Detection Tools & Trend Analysis

The GRACE system is combined with an automated search tool for investigative evidence.[291] This search tool also relies on digital identifiers for the detection of CSA material known from the CSEM reports. These digital identifiers could help to inform the EU Centre when generating relevant indicators for the database of indicators for known CSA material, and when compiling the list of URLs indicating specific items of CSA material hosted by a provider not offering services in the EU.

Furthermore, the search tool developed for and integrated in the GRACE system could perhaps contribute to facilitate the Coordinating Authorities' investigatory powers also include the power to monitor compliance

[290] ETL = Extract, Transform, Load; referring to the general procedure of copying data from one or more sources into a destination system which represents the data differently from the source(s) or in a different context than the source(s), see: https://en.wikipedia.org/wiki/Extract,_transform,_load.
[291] For details and the differentiation between searches in individual investigations and general searches for CSE content see Deliverable D9.1., section 4.

with the Draft Regulation Against Online CSA by conducting searches on publicly accessible material to detect known or new CSA material.

Finally, the GRACE tools developed for the predictive analysis of trends in CSE offenders' tactics could perhaps support the EU Centre's role as information and expertise hub[292].

[292] Art. 50(2) and (3) Draft Regulation Against Online CSA.

5. EU-Proposal for a Regulatory Framework Governing AI

This chapter takes a closer look at the regulatory framework for artificial intelligence proposed by the European Commission in April 2021 and provides a first analysis how this future regulatory framework will apply to the tools and platform developed in the course of the GRACE project.

On 21 April 2021, the European Commission presented a legislative package addressing both policy dimensions of AI[293] because the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society.[294] In an effort to strengthen AI uptake, investment and innovation across the EU, the European Commission made a revised Coordinated Plan on AI[295] available. In order to address the potential high risks AI poses to safety and fundamental rights, the European Commission presented the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).[296] As first-ever legal framework on AI, the Artificial Intelligence Act is complemented by a proposal for a Regulation on Machinery Products[297] adapting safety rules to increase users' trust in the new, versatile generation of products.

First, the objectives and the risk-based approach of the proposed Artificial Intelligence Act are presented (section 5.1. below). Second, it is examined how the Artificial Intelligence Act classifies and regulates the GRACE tools and platform (section 5.2. below). Finally, the diverging approaches of the European Parliament and of the Council to core concepts of the Artificial Intelligence Act are outlined (section 5.3 below).

5.1. Objectives and Approach of the Artificial Intelligence Act

The new regulatory framework for AI strives to achieve *four specific objectives*: (i) ensure that AI systems are safe and respect existing law on fundamental rights and Union values; (ii) ensure legal certainty; (iii) enhance governance and effective enforcement of existing law on fundamental rights and safety; and (iv) facilitate the development of a single market for lawful, safe and trustworthy AI applications.[298] For this purpose, the Artificial Intelligence Act sets harmonised rules for the development, placement and use of AI systems in the

[293] Starting with the launch of the European AI strategy in April 2018, the Commission's two-pronged policy has been to make the EU a world-class hub for AI, while ensuring that AI is human-centric and trustworthy. See Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 19 February 2020, setting out as vision for AI in Europe: an ecosystem of excellence and an ecosystem of trust for AI.

[294] Commission, Communication: Fostering a European approach to artificial intelligence, COM(2021) 205 final, 21 April 2021, p. 1.

[295] Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, 21 April 2021.

[296] Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, 21 April 2021.

[297] Commission, Proposal for a Regulation of the European Parliament and of the Council on machinery products, COM(2021) 202 final, 21 April 2021.

[298] Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, 21 April 2021, p. 3.

EU.

Following a *risk-based approach,* certain particularly harmful AI practices are *prohibited* and *specific restrictions and safeguards* are placed on law enforcement's use of remote biometric identification systems,[299] while *high-risk AI systems*[300] posing significant risks to the health and safety or fundamental rights of individuals have to comply with a set of horizontal mandatory requirements for trustworthy AI[301] and follow conformity assessment procedures[302]. Complementing the technological requirements, the Artificial Intelligence Act also sets out obligations on each and every provider and user of a high-risk AI system to ensure safety and respect for fundamental rights throughout the entire lifecycle of an AI system.[303] Regarding *non-high-risk AI systems*, their providers are encouraged to draw up codes of conduct fostering the voluntarily application of the requirements for trustworthy AI.[304]

This risk methodology reveals that the requirements for trustworthy AI set out in Chapter 2 of the Artificial Intelligence Act are a crucial feature for AI systems in the EU. This set of specifically designed requirements echoes the criteria elaborated in the H-LEG's "Ethical Guidelines for Trustworthy AI"[305] which are examined for the GRACE tools and platform in Deliverable D9.1.[306] Chapter 2 of the Artificial Intelligence Act requires the operation of a risk management system,[307] the use of high-quality datasets,[308] the establishment of appropriate documentation[309] to enhance traceability,[310] the sharing of adequate information with the user,[311] the design and implementation of appropriate human oversight measures,[312] and the achievement of the highest standards in terms of robustness, safety, cybersecurity and accuracy.[313]

5.2. Application to GRACE Tools and Platform

5.2.1. Scope of the Artificial Intelligence Act

The tools and platform developed in the course of the GRACE project (GRACE system) fall under the proposed Artificial Intelligence Act. Art. 3(1) Artificial Intelligence Act defines an AI system as software that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations or decisions influencing the environments they interact with. Further, the software has to be developed with at least one of the techniques and approaches listed in Annex I which contains (a) machine learning approaches,

[299] Art. 5 Artificial Intelligence Act.
[300] Art. 6 Artificial Intelligence Act.
[301] Art. 8(1) Artificial Intelligence Act demanding compliance with all requirements of Chapter 2 Artificial Intelligence Act.
[302] Art. 43 Artificial Intelligence Act.
[303] See Artt. 16 – 29 Artificial Intelligence Act (Chapter 3).
[304] Art. 69 Artificial Intelligence Act.
[305] AI H-LEG, "Ethics Guidelines for Trustworthy AI", 8 April 2019.
[306] See section 3. of Deliverable 9.1 Ethical Report.
[307] Art. 9 Artificial Intelligence Act.
[308] Art. 10 Artificial Intelligence Act.
[309] Art. 11 Artificial Intelligence Act.
[310] Art. 12 Artificial Intelligence Act.
[311] Art. 13 Artificial Intelligence Act.
[312] Art. 14 Artificial Intelligence Act.
[313] Art. 15 Artificial Intelligence Act.

(b) logic- and knowledge-based approaches, and (c) statistical approaches, Bayesian estimation, search and optimisation methods.

ANNEX I – ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3(1)

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods.

This definition of AI is technology-neutral and, according to Art. 4 Artificial Intelligence Act, open to be updated by the European Commission in line with (future) market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed in Annex I. This definition is also significantly broader than the definition of AI elaborated by the High-Level Expert Group on AI in 2018,[314] because the definition suggested in the Artificial Intelligence Act appears to lack the element of unpredictability as well as the element of a black box effect. Therefore, this definition of AI appears to comprise not only deterministic software but also traditional expert systems.[315]

The GRACE project develops Big Data solutions for data ETL[316] which will not only standardise the management of CSEM reports, but also avoid duplicate processing and enhance collaboration amongst national LEAs within the EU. The data of each CSEM report will be analysed in terms of visual, audio and text information using AI technologies to produce structured and validated information from the CSEM report's content. For this purpose, GRACE will develop novel forensic analysis tools for (i) CSEM-specific content analysis and classification, (ii) content-based geo-localisation, (iii) the creation of evidence graphs to connect cases, (iv) case prioritisation techniques and (v) predictive analysis of trends in CSE offenders' tactics. For the operational coordination of LEAs in all Member States, a Federated (Machine) Learning platform will be developed and established which will exploit available infrastructure as well as the metadata of any CSEM content distributed across the entire EU. As a consequence, the entire GRACE system qualifies as AI system within the meaning of the Artificial Intelligence Act independent of the question whether the GRACE system would be combined with an automated search tool for investigative evidence[317] or not.

[314] High-Level Expert Group on AI, "A Definition of AI: Main Capabilities and Disciplines", 8 April 2019, page 6.

[315] Spindler, "Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung von Künstlicher Intelligenz", Computer und Recht 2021, page 361.

[316] ETL = Extract, Transform, Load; referring to the general procedure of copying data from one or more sources into a destination system which represents the data differently from the source(s) or in a different context than the source(s), see: https://en.wikipedia.org/wiki/Extract,_transform,_load.

[317] For details and the differentiation between searches in individual investigations and general searches for CSE content see Deliverable D9.1., section 4.

5.2.2. High-Risk AI System

The specific restrictions and safeguards set out in Art. 5(1)(d) Artificial Intelligence Act for the use of 'remote biometric identification systems'[318] for the purpose of law enforcement would not be applicable. First, the identification system developed in the course of the GRACE system seems unlikely to be operated for 'real time' identifications and, second, online spaces do not qualify as 'publicly accessible spaces' within the meaning of Art. 3(39) Artificial Intelligence Act because they are not physical spaces.[319]

The GRACE system falls squarely under the definition of a *high-risk AI system* established in Art. 6(2) Artificial Intelligence Act in connection with Annex III No. 1 listing any AI system for remote biometric identification of natural persons[320] as well as No. 6 regarding the area of law enforcement listing explicitly AI systems intended to be used by LEAs for the evaluation of the reliability of evidence,[321] profiling in the course of an investigation,[322] and Big Data applications[323]. These AI systems intended to be used in the law enforcement context have been classified as high-risk because their accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress.[324]

> ***Article 6 – Classification rules for high-risk AI systems***
>
> *1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:*
>
> *(a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;*
>
> *(b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.*
>
> *2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.*
>
> ***ANNEX III – HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)***
>
> *High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:*
>
> *1. Biometric identification and categorisation of natural persons:*
>
> *(a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of*

[318] Defined in Art. 3(36) Artificial Intelligence Act as an AI system for the purpose of identifying natural persons through the comparison of a person's biometric data with the biometric data contained in a reference database.
[319] Recital 9 sentence 3 Artificial Intelligence Act.
[320] 'real time' and 'post'.
[321] Annex III No. 6(d) Artificial Intelligence Act.
[322] Annex III No. 6(f) Artificial Intelligence Act.
[323] Annex III No. 6 (g) Artificial Intelligence Act.
[324] Recital 38 sentence 4 Artificial Intelligence Act.

natural persons;

2. Management and operation of critical infrastructure:

(a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.

3. Education and vocational training:

(a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;

(b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.

4. Employment, workers management and access to self-employment:

(a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;

(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behaviour of persons in such relationships.

5. Access to and enjoyment of essential private services and public services and benefits:

(a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;

(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;

(c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.

6. Law enforcement:

(a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;

(b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

(c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);

(d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;

(e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;

(f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;

(g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

7. Migration, asylum and border control management:

(a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

(b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

(c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;

(d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

8. Administration of justice and democratic processes:

(a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

As *high-risk AI system*, the GRACE system will have to be registered in the EU database for *stand-alone high-risk AI systems* established by Art. 60 Artificial Intelligence Act before the GRACE system could be placed on the market or put into service.[325]

Update for Legal Report v2:

For the registration according to Art. 51 Artificial Intelligence Act, a *high-risk AI system* has to comply with the seven mandatory requirements established in Title III. Chapter 2 of the Artificial Intelligence Act:

(1) the operation of a *risk management system*,[326]

(2) the use of *high-quality datasets*,[327]

(3) the establishment of *appropriate documentation,*[328]

(4) the inclusion of *logging capabilities* to enhance traceability,[329]

[325] Art. 51 Artificial Intelligence Act.
[326] Art. 9 Artificial Intelligence Act.
[327] Art. 10 Artificial Intelligence Act.
[328] Art. 11 Artificial Intelligence Act.
[329] Art. 12 Artificial Intelligence Act.

(5) the sharing of *adequate information* with the end-user,[330]

(6) the design and implementation of *appropriate human oversight measures*,[331] and

(7) the achievement of the highest standards in terms of *robustness*, *safety*, *cybersecurity* and *accuracy*.[332]

The compliance of a *high-risk AI system* with these requirements would be evaluated in the mandatory conformity assessment procedure.[333] Once the conformity assessment has demonstrated the *high-risk AI system's* compliance with the requirements set out in Title III. Chapter 2 of the Artificial Intelligence Act, an *EU declaration of conformity* can be drawn up[334] and a *CE marking of conformity* can be affixed[335].

The provider of a *high-risk AI system* has to fulfil all obligations established in Art. 16 Artificial Intelligence Act. These obligations serve to ensure the compliance of the *high-risk AI system* with the Artificial Intelligence Act throughout its lifecycle. In addition to ensuring that the *high-risk AI system* is compliant with the requirements set out in Title III. Chapter 2 Artificial Intelligence Act,[336] it is also necessary to:

- put in place a *quality management system* in accordance with Art. 17 Artificial Intelligence Act,[337]
- provide the *technical documentation* of the *high-risk AI system*,[338] and
- keep the *logs* automatically generated by the *high-risk AI system*.[339]

The user of a *high-risk AI system* is, pursuant to Art. 29(1) Artificial Intelligence Act, merely obliged to use the *high-risk AI system* in accordance with the instructions of use accompanying the system. Whether the user organises its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider, is left to the user's discretion.[340] Only to the extent that the user exercises control over the input data, the user shall ensure that the input data is relevant in view of the intended purpose of the *high-risk AI system*.[341] However, users have the obligation to monitor the operation of the *high-risk AI system* on the basis of the instructions of use and must suspend the use and notify the provider or distributor in cases of serious incidents or malfunctions and in case a risk at national level is posed.[342]

5.2.3. Deviating Approaches by Parliament and Council

The legislative process for a future Artificial Intelligence Act is still pending. After the proposal of the Artificial Intelligence Act by the European Commission in April 2021, the Slovenian Presidency of the Council had

[330] Art. 13 Artificial Intelligence Act.
[331] Art. 14 Artificial Intelligence Act.
[332] Art. 15 Artificial Intelligence Act.
[333] Art. 19(1) Artificial Intelligence Act.
[334] Art. 48 Artificial Intelligence Act.
[335] Art. 49 Artificial Intelligence Act.
[336] Art. 16(a) Artificial Intelligence Act.
[337] Art. 16(b) Artificial Intelligence Act.
[338] Art. 16(c) Artificial Intelligence Act.
[339] Art. 16(d) Artificial Intelligence Act.
[340] Art. 29(2) Artificial Intelligence Act.
[341] Art. 29(3) Artificial Intelligence Act.
[342] Art. 29(4) Artificial Intelligence Act.

presented an early compromise text in November 2021[343] and the European Parliament's Committee on Internal Market and Consumer Protection and its Committee on Civil Liberties, Justice and Home Affairs jointly presented their Draft Report in April 2022 (section 5.2.3.1 below). Whereas the joint committee procedure in the European Parliament continues to deal with, by now, more than 3,000 suggested amendments to the Draft Report,[344] the Council was able to adopt its General Approach in December 2022 (section 5.2.3.2 below).

This section points out the deviating approaches to key elements of the future Artificial Intelligence Act which are most relevant for the development of the GRACE system and most likely will have to be resolved in the final trilogue phase, once the position of the European Parliament has been agreed upon – currently expected for summer 2023. If the trilogue phase was to begin this summer, then the final legal framework for the development of *AI systems* could be expected to come into force in the first half of 2024.

5.2.3.1. Parliament's Initial Draft Report

In the ordinary legislative procedure (COD) the next step after a proposal by the European Commission is for the European Parliament to adopt its position. However, already the briefing provided by the European Parliamentary Research Service for the European Parliament revealed that the final shape of a future Artificial Intelligence Act is highly controversial among national parliaments, stakeholders and academics.[345] the *Committee on Internal Market and Consumer Protection* (IMCO) and the *Committee on Civil Liberties, Justice and Home Affairs* (LIBE) presented their joint Draft Report in April 2022 suggesting more than three hundred amendments (Amended AI Act) to the Artificial Intelligence Act.[346] This initial Draft Report has received more than 3,000 suggested amendments which currently are being considered.[347]

[343] Council of the EU, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text, 2021/0106(COD), 29 November 2021, available at: https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf.

[344] See https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence (last visited on 18 February 2023); Bertuzzi, "AI regulation filled with thousands of amendments in the European Parliament", EURACTIVE, 2 and 7 June 2022, available at: https://www.euractiv.com/section/digital/news/ai-regulation-filled-with-thousands-of-amendments-in-the-european-parliament/.

[345] European Parliament Research Service (EPRS), Briefing on EU Artificial Intelligence Act as Legislation in Progress by Tambiama Madiega, PE 698.792 – November 2021, available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf.

[346] European Parliament, Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM2021/0206 – C9-0146/2021 – 2021/0106(COD)), 20 April 2022 by Rapporteur: Brando Benifei and Ioan-Dragoş Tudorache suggesting 309 amendments to the Artificial Intelligence Act.

[347] See https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence (last visited on 18 February 2023).

Whereas the *European Economic and Social Committee*[348] and the *Committee of the Regions*[349] had issued their opinions in 2021, most committees of the European Parliament have adopted their opinion in the course of 2022: *Committee on the Environment, Public Health and Food Safety* (ENVI),[350] *Committee on Industry, Research and Energy* (ITRE),[351] *Committee on Culture and Education* (CULT),[352] *Committee on Transport and Tourism* (TRAN),[353] and *Committee on Legal Affairs* (JURI).[354]

For the purposes of highlighting European Parliament's tendency to deviate from three key elements of the Commission's proposal, this section solely relies on the initial Draft Report as preliminary indication of the position of the European Parliament, because this initial Draft Report contains the points on which the co-Rapporteurs could easily agree and touches upon all the main elements of the Artificial Intelligence Act.

- **Definition of *AI system***

In general, Parliament's Draft Report takes the view that no *AI system* as such should be excluded ex-ante from the definition of "artificial intelligence" and suggests for Art. 3(1) Artificial Intelligence Act to delete the requirement that the set of objectives given to an *AI system* has to be "human-defined" and to add mere "hypotheses" in the list of potential outputs generated by an *AI system*.[355]

- **Obligations for the user of an *AI system***

Regarding the use of a *high-risk AI system*, Parliament's Draft Report would introduce the obligation for a LEA using the GRACE system as user to appoint competent persons responsible for the human oversight of the *high-risk AI system.*

Parliament's Draft Report takes the view that users should play a more active role in reporting cases of incidents or malfunctioning of *high-risk AI systems* because the user is sometimes better placed to spot such incidents or malfunctions.[356] Therefore, the Draft Report suggests to insert new and additional paragraphs

[348] European Economic and Social Committee (EESC), Opinion on AI/Regulation, 22 September 2021, Rapporteur: Catelijne Muller, available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/regulation-artificial-intelligence.
[349] European Committee of the Regions, European Approach to Artificial Intelligence – Artificial Intelligence Act (Revised Opinion), 2 December 2021, Rapporteur: Guido Rink, available at: https://cor.europa.eu/EN/our-work/Pages/OpinionTimeline.aspx?opId=CDR-2682-2021.
[350] Committee on the Environment, Public Health and Food Safety (ENVI), Opinion on AI Act, 22 April 2022, Rapporteur: Susana Solís Pérez, available at: https://www.europarl.europa.eu/doceo/document/ENVI-AD-699056_EN.pdf.
[351] Committee on Industry, Research and Energy (ITRE), Opinion on AI Act, 14 June 2022, Rapporteur: Eva Maydell, available at: https://www.europarl.europa.eu/doceo/document/ITRE-AD-719801_EN.pdf.
[352] Committee on Culture and Education (CULT), Recommendations for AI Act, 15 June 2022, Rapporteur: Marcel Kolaja, available at: https://www.europarl.europa.eu/news/en/press-room/20220613IPR32821/ai-act-meps-add-their-recommendations-for-culture-and-education.
[353] Committee on Transport and Tourism (TRAN), Opinion on AI Act, 12 July 2022, Rapporteur: Josianne Cutajar, available at: https://www.europarl.europa.eu/doceo/document/TRAN-AD-730085_EN.pdf.
[354] Committee on Legal Affairs (JURI), Opinion on AI Act, 2021/0106(COD), 12 September 2022, Rapporteur: Axel Voss, available at: https://www.europarl.europa.eu/doceo/document/JURI-AD-719827_EN.html.
[355] Amendment 55 in European Parliament, Draft Report on Artificial Intelligence Act, (COM2021/0206 – C9-0146/2021 – 2021/0106(COD)), 20 April 2022, p. 45 et seq.
[356] European Parliament, Draft Report on Artificial Intelligence Act, (COM2021/0206 – C9-0146/2021 – 2021/0106(COD)), 20 April 2022, p. 160.

after Art. 29(1) Artificial Intelligence Act introducing for users of *high-risk AI systems* the obligation to comply with the human oversight requirements (1a) and requiring the assignment of a competent and properly qualified and trained natural person responsible for this compliance who has the necessary resources to ensure the necessary supervision of the *AI system* (1b) and (1c).[357] The aim of these suggestions is to increase democratic oversight, public scrutiny and accountability for any public authority, Union institution, agency or body leading to more transparency towards the public on the use of AI systems in sensitive areas impacting upon people's lives.[358]

5.2.3.2. Council's General Approach

On 6 December 2022, the Council of the EU adopted its General Approach[359] to the future Artificial Intelligence Act.

- **Definition of *AI system***

The Council's General Approach suggests to define the notion of an *AI system* in a different and to some extent broader way. According to Art. 3(1) General Approach AI Act, an *AI system* refers to a "system" (!) that is "designed to operate with elements of autonomy" and that has two specific capabilities: first, an *AI system* "infers how to achieve a given set of objectives" and second, it "produces system-generated outputs such as content (*generative AI systems*), predictions, recommendations or decisions, influencing the environments with which the *AI system* interacts". Both capabilities are "based on machine and/or human-provided data and inputs" and involve "using machine learning and/or logic- and knowledge-based approaches". As a consequence, the focus of what constitutes an *AI system* has shifted in the General Approach on the overall system. With the explicit inclusion of "autonomy" as a characteristic feature of an *AI system* and the emphasis on an *AI system's* interaction with its environment, an *AI system* under the General Approach is not limited to software, but also includes machines, robots and any other system combining digital and physical components equipped with such an element of autonomy.[360]

The entire envisioned GRACE system including the physical components for input and well as for output would constitute an *AI system* according to this wider definition of *AI system* in the General Approach.

- **Risk Classification**

For the classification of an *AI system* as *high-risk* established in Art. 6(3) General Approach AI Act in connection with Annex III of the General Approach AI Act, the General Approach simplifies the Commission's approach to "biometric identification and categorisation of natural persons" to addressing merely "biometrics" and including any "remote biometric identification system" in No. 1(a) of the Annex III. In deviation from the

[357] Amendments 136, 137 and 138 in European Parliament, Draft Report on Artificial Intelligence Act, (COM2021/0206 – C9-0146/2021 – 2021/0106(COD)), 20 April 2022, p. 79.
[358] European Parliament, Draft Report on Artificial Intelligence Act, (COM2021/0206 – C9-0146/2021 – 2021/0106(COD)), 20 April 2022, p. 160.
[359] Council, General Approach AI Act, no. 15698/22 on interinstitutional file 2021/0106(COD), 6 December 2022, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15698_2022_INIT&from=EN.
[360] Borges, „Liability for AI Systems Under Current and Future Law", Computer Law Review International (CRi) 2023, p. 1 (p. 2 at para. 10).

Commission's Proposal, the Council's General Approach also suggests to extend the *high-risk* classification of AI systems intended for the evaluation of the reliability of evidence in No. 6(d) of the Annex III as well as AI systems intended for profiling natural persons in the course of an investigation in No. 6(f) of the Annex III from the use by LEAs themselves to explicitly include any use "on their behalf" as well. Finally, the General Approach does not classify AI systems intended for Big Data applications in the context of "crime analytics regarding natural persons" any more as *high-risk* per se and suggests to delete No. 6(g) of the Annex III.

- **Obligations for the user of an *AI system***

Regarding the use of a *high-risk AI system*, Art. 29(1a) General Approach AI Act would introduce the additional obligation for a LEA using the GRACE system as *user* to assign human oversight to a natural person who has the necessary competence, training and authority.

6. Victims' Rights

Child sexual abuse and exploitation (CSE) is a particularly heinous crime that has wide-ranging and serious life-long consequences for victims. In hurting children, these crimes also cause significant and long-term social harm. Respect for human dignity is the foundation of human rights. CSE is a gross violation of the children's right to respect for their human dignity and physical and mental integrity.

This chapter provides an overview of the legal frameworks established in international treaties at global level by the United Nations (section 6.1. below) and at regional level by the Council of Europe (section 6.2. below) as well as of the legal framework for victims' rights within the European Union (section 6.3. below).[361]

6.1. United Nations Framework

The provisions of the Universal Declaration of Human Rights[362] and all other international human rights treaties including those of the International Covenant on Civil and Political Rights[363] also apply to children. However, it was not until the drafting and near universal ratification of a human rights convention enshrining the comprehensive set of rights held by children that the distinct characteristics of childhood have gained international recognition. Under the Convention on the Rights of the Child (CRC),[364] a child is explicitly recognised as a human rights holder entitled to non-negotiable rights to protection. The child is entitled to all human rights and fundamental freedoms laid down in the CRC and related international human rights instruments and jurisprudence.

6.1.1. Child Protection Rights

At global level, the CRC is the cornerstone of children's rights imposing legally binding obligations on States Parties to respect, protect and fulfil the rights of the child. There are specific protection rights in the CRC which include protection from all forms of child abuse, neglect, exploitation and cruelty before a child falls victim to any of these. While Art. 34 CRC explicitly requires States Parties to protect children from all forms of sexual exploitation and abuse, Art. 19 CRC obligates the States Parties in a much broader sense to prohibit, prevent and respond to all forms of violence, injury or abuse, maltreatment or exploitation of children, including sexual abuse, while in the care of parents or any other legal guardian.[365] For children who have become a victim, the

[361] For an initial presentation of the main legal bases in relation to child protection against sexual abuse and exploitation see also section 5. of Deliverable D10.6.
[362] United Nations, General Assembly, Universal Declaration of Human Rights (UDHR), Resolution 217 A, A/RES/3/217 A, 10 December 1948.
[363] United Nations, International Covenant on Civil and Political Rights, Resolution 2200A (XXI), adopted on 16 December 1966, entered into force on 23 March 1976.
[364] United Nations, Convention on the Rights of the Child (CRC), Resolution 44/25, adopted on 20 November 1989, entered into force on 2 September 1990; the CRC is the most ratified human rights treaty in the world because all UN Member States (except the USA) have agreed to be bound by the obligation to uphold children's rights in all spheres of life.
[365] Violence within the meaning of Art. 19(1) CRC includes any form of CSEM as violence through information and communications technologies; see: UN Committee on the Rights of the Child, General

States Parties have to take protective measures including effective procedures for the investigation and treatment of instances of child maltreatment as well as for judicial involvement.[366]

> ***Article 19 CRC***
>
> *1. States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child.*
>
> *2. Such protective measures should, as appropriate, include effective procedures for the establishment of social programmes to provide necessary support for the child and for those who have the care of the child, as well as for other forms of prevention and for identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment described heretofore, and, as appropriate, for judicial involvement.*

> ***Article 34 CRC***
>
> *States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:*
>
> *(a) The inducement or coercion of a child to engage in any unlawful sexual activity;*
>
> *(b) The exploitative use of children in prostitution or other unlawful sexual practices;*
>
> *(c) The exploitative use of children in pornographic performances and materials.*

These protective measures require a *child rights approach* furthering the realisation of the rights of all children as set out in the CRC. The States Parties are obligated to develop the capacity of duty bearers to meet their obligations to respect, protect and fulfil rights (Art. 4 CRC) and the capacity of rights holders to claim their rights. This child rights approach has to be guided at all times by the rights to *non-discrimination* (Art. 2 CRC), consideration of the *best interests of the child* (Art. 3(1) CRC), *life, survival and development* (Art. 6 CRC), and *respect for the views of the child* (Art. 12 CRC). Furthermore, children have the right to be directed and guided in the exercise of their rights by caregivers, parents and community members, in line with children's evolving capacities (Art. 5 CRC).[367]

6.1.2. Child Victim's Rights

The position of a child as victim is explicitly recognised in Art. 39 CRC. This provision requires States Parties to

comment No. 13 (2011) on the right of the child to freedom from all forms of violence, 18 April 2011, CRC/C/GC/13, at para. 31.

[366] Art. 19(2) CRC.

[367] See the definition of a child rights approach in: UN Committee on the Rights of the Child, General comment No. 13 (2011) on the right of the child to freedom from all forms of violence, 18 April 2011, CRC/C/GC/13, at para. 59.

take all appropriate measures to promote physical and psychological recovery and social reintegration of child victims (sentence 1). This recovery and reintegration must take place in an environment which fosters the health, self-respect and dignity of the child (sentence 2). For that reason, Art. 19(2) CRC requires appropriate "investigation" and "treatment" among several other services needed for child victims.

> ***Article 39 CRC***
>
> *States Parties shall take all appropriate measures to promote physical and psychological recovery and social reintegration of a child victim of: any form of neglect, exploitation, or abuse; torture or any other form of cruel, inhuman or degrading treatment or punishment; or armed conflicts. Such recovery and reintegration shall take place in an environment which fosters the health, self-respect and dignity of the child.*

While the investigation of instances of violence requires a child rights-based and child-sensitive approach by qualified professionals,[368] the appropriate "treatment" of a child victim must pay heed to: (i) inviting and giving due weight to the child's views; (ii) the safety of the child; (iii) the possible need for her or his immediate safe placement; and (iv) the predictable influences of potential interventions on the child's long-term well-being, health and development. In this respect, a full range of services should be available upon identification of abuse, ranging from medical, mental health, social and legal services and support as well as longer term follow-up services including family group conferencing and other similar practices.[369]

All judicial proceedings involving child victims of violence must not only adhere to the celerity principle while respecting the rule of law, but also treat the child victim in a child-friendly and sensitive manner throughout the justice process, taking into account the child's personal situation, needs, age, gender, disability and level of maturity and fully respecting their physical, mental and moral integrity.[370] The UN Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime provide very detailed guidance on how to implement these aspects in the areas starting with the guiding principles (at III.) over to specifying the impact of: the right to be treated with dignity and compassion (at V.), the right to be protected from discrimination (at VI.), the right to be informed (at VII.), the right to be heard and to express views and concerns (at VIII.), the right to effective assistance (at IX.), the right to privacy (at X.), the right to be protected from hardship during the justice process (at XI.), the right to safety (XII.), as well as the right to reparation (XIII.) and the right to special preventive measures (XIV.).[371]

Regarding victims of CSE, the CRC has been augmented by the Optional Protocol on the sale of children, child

---

[368] UN Committee on the Rights of the Child, General comment No. 13 (2011) on the right of the child to freedom from all forms of violence, 18 April 2011, CRC/C/GC/13, at para. 51.
[369] UN Committee on the Rights of the Child, General comment No. 13 (2011) on the right of the child to freedom from all forms of violence, 18 April 2011, CRC/C/GC/13, at para. 52.
[370] UN Committee on the Rights of the Child, General comment No. 13 (2011) on the right of the child to freedom from all forms of violence, 18 April 2011, CRC/C/GC/13, at para. 54(b) and (d); UN Economic and Social Council (ECOSOC), Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, 22 July 2005, Annex to Resolution 2005/20, especially at 10. – 14.
[371] UN Economic and Social Council (ECOSOC), Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, Annex to Resolution 2005/20, 22 July 2005. Regarding the interpretation of the right to be informed (at VII.) and the right to be heard (at VIII.) see also: UN Committee on the Rights of the Child (2009), General Comment no. 12 (2009): The right of the child to be heard, CRC/C/GC/12, 1 July 2009, at paras. 62 et seq.

prostitution and child pornography.[372] Art. 8(1) of this Optional Protocol obligates States Parties to adopt appropriate measures to protect the rights and interests of child victims at all stages of the criminal justice process. A key guiding principle is enshrined in Art. 3(1) CRC and requires States Parties to ensure that *"the best interests of the child"* are a primary consideration of all state activities (including courts of law and law enforcement activities) in all actions concerning children. The full application of the concept of the *child's best interests* is inherently intertwined with the *child rights approach* engaging all actors to secure the child's holistic integrity and human dignity.[373] Achieving this requires the cooperation of a broad range of institutions and actors, and the United Nations Model Strategies and Practical Measures on the Elimination of Violence against Children in the Field of Crime Prevention and Criminal Justice identify the "complementary roles of the criminal justice system, child protection agencies, health, education and social service sectors and, in some cases, informal justice systems in creating a protective environment and preventing and responding to incidents of violence against children".[374]

6.2. CoE Framework

In the European regional frame, the Council of Europe (CoE) is an international organisation based on cooperation causing the efficacy of its action to rely on the political will of its States Parties. This means that the efficacy of a convention's objectives, in principle, depends not only on the ratification of the treaty by the States Parties of the Council of Europe but also on the adoption of all national measures necessary to implement the treaty by the relevant States Parties.[375]

6.2.1. Convention No. 116 on the Compensation of Victims of Violent Crimes

The CoE established the protection of victims' rights with the European Convention on the Compensation of Victims of Violent Crimes adopted on 24 November 1983 (Convention No. 116).[376] Convention No. 116 deals, on the one hand, with victims of intentional crimes who have suffered bodily injury or impairment of health and of dependants of persons who have died as a result of such crimes. On the other hand, Convention N. 116 deals with the need to introduce schemes for compensation for these victims by the state in whose territory

[372] United Nations, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, A/RES/54/263, adopted on 16 March 2001, entered into force on 18 January 2002.
[373] UN Committee on the Rights of the Child, General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1), CRC/C/GC/14, 29 March 2013, at para. 5.
[374] United Nations, 2014, GA Resolution A/RES/69/194, adopted on 18 December 2014, 26 January 2015, Annex at para 23.
[375] Fernández de Casadevante Romani in: von Bogdandy/Wolfrum (eds.), Max Planck Yearbook of United Nations Law, Vol. 14, 2010, p. 219 (p. 231).
[376] CoE, Convention on the Compensation of Victims of Violent Crimes, Convention No. 116, adopted on 24 November 1983, entered into force on 1 February 1988.

the crime was committed,[377] in particular when the offender has not been identified or is without resources.[378]

According to Art. 3 Convention No. 116, two groups of victims are eligible to compensation: (i) nationals of the States Parties to the Convention and (ii) nationals of all Member States of the Council of Europe who are permanent residents in the state on whose territory the crime was committed. As a result of this approach, three groups of victims are excluded from a possible compensation: (i) the nationals of all Member States of the Council of Europe that are not States Parties to the Convention; (ii) the nationals of all Member States of the Council of Europe that are not permanent residents in the state on whose territory the crime was committed; and (iii) the nationals of third states.

Article 3 Convention No. 116

Compensation shall be paid by the State on whose territory the crime was committed:

a. to nationals of the States party to this Convention;

b. to nationals of all member States of the Council of Europe who are permanent residents in the State on whose territory the crime was committed.

Article 4 Convention No. 116

Compensation shall cover, according to the case under consideration, at least the following items: loss of earnings, medical and hospitalisation expenses and funeral expenses, and, as regards dependants, loss of maintenance.

Article 5 Convention No. 116

The compensation scheme may, if necessary, set for any or all elements of compensation an upper limit above which and a minimum threshold below which such compensation shall not be granted.

Article 6 Convention No. 116

The compensation scheme may specify a period within which any application for compensation must be made.

Article 7 Convention No. 116

Compensation may be reduced or refused on account of the applicant's financial situation.

Article 8 Convention No. 116

(1) Compensation may be reduced or refused on account of the victim's or the applicant's conduct before, during or after the crime, or in relation to the injury or death.

(2) Compensation may also be reduced or refused on account of the victim's or the applicant's involvement in organised crime or his membership of an organisation which engages in crimes of violence.

(3) Compensation may also be reduced or refused if an award or a full award would be contrary to a sense of justice or to public policy (ordre public).

The scope of the victim's compensation shall cover at least loss of earnings, medical and hospitalisation

[377] Art. 3 Convention No. 116.
[378] Art. 2 Convention No. 116.

expenses and funeral expenses.[379] However, Convention No. 116 allows States Parties not only to set for any element of compensation, if necessary, an upper limit,[380] but also to reduce or refuse victim's compensation in four situations: (i) on account of the applicant's financial situation;[381] (ii) on account of the victim's or the applicant's conduct before, during or after the crime;[382] (iii) on account of the victim's involvement in organised crime;[383] or (iv) if awarding compensation would be contrary to a sense of justice or to public policy (*ordre public*).

6.2.2. Lanzarote Convention

While the CoE Convention on Action against Trafficking in Human Beings (Convention No. 197)[384] already highlights particular needs of child victims in the context of all forms of trafficking in human beings for sexual exploitation,[385] the first instrument to establish the various forms of sexual abuse of children as criminal offences is the CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)[386]. Art. 31 Lanzarote Convention indicates which general measures of protection States Parties should take to protect the rights and interests of victims, including their special needs as witnesses, at all stages of investigations and criminal proceedings. These measures include (i) informing child victims of their rights and the services at their disposal,[387] (ii) enabling child victims to be heard and to supply evidence,[388] (iii) providing child victims with appropriate support services so that their rights and interests are duly presented and taken into account,[389] (iv) protecting their privacy, their identity and their image,[390] (v) providing for their safety from intimidation, retaliation and repeat victimisation,[391] (vi) ensuring that contact between child victims and perpetrators within court and LEA premises is avoided.[392] In addition, Art. 31 Lanzarote Convention provides that child victims must have access to legal aid.[393] At any stage, the information provided must be adapted to child victim's age and maturity and be in a language which the child victim

[379] Art. 4 Convention No. 116.
[380] Art. 5 Convention No. 116.
[381] Art. 7 Convention No. 116.
[382] Art. 8(1) Convention No. 116.
[383] Art. 8(2) Convention No. 116.
[384] CoE, Convention on Action against Trafficking in Human Beings, Convention No. 197, adopted on 16 May 2005, entered into force on 1 February 2008.
[385] Convention No. 197 aims to design a comprehensive framework for the protection and assistance of victims, Art. 1(1)(b). For child victims, Convention No. 197 includes particular measures e.g. for their identification, Art. 10(4), for assistance in their physical, psychological and social recovery, Art. 12(1) and (7), and repatriation, Art. 16(7). Further, Convention No. 197 ensures that the child victim is afforded special protection measures taking into account the child's best interests before and during court proceedings, Art. 28 (3) and Art. 30.
[386] CoE, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Convention No. 201, adopted on 25 October 2007, entered in to force on 1 July 2010.
[387] Art. 31(1)(a) Lanzarote Convention.
[388] Art. 31(1)(c) Lanzarote Convention.
[389] Art. 31(1)(d) Lanzarote Convention.
[390] Art. 31(1)(e) Lanzarote Convention.
[391] Art. 31(1)(f) Lanzarote Convention.
[392] Art. 31(1)(g) Lanzarote Convention.
[393] Art. 31(3) Lanzarote Convention.

understands.[394]

The Lanzarote Convention contains also requirements safeguarding interviews of a child victim against delays, child-unfriendly premises or unprofessional interviewers,[395] and ensuring that hearings of a child victim in criminal court proceedings can either take place without the presence of the public or victim may be heard in the courtroom without being physically present.[396]

Article 31 Lanzarote Convention – General measures of protection

(1) Each Party shall take the necessary legislative or other measures to protect the rights and interests of victims, including their special needs as witnesses, at all stages of investigations and criminal proceedings, in particular by:

a. informing them of their rights and the services at their disposal and, unless they do not wish to receive such information, the follow-up given to their complaint, the charges, the general progress of the investigation or proceedings, and their role therein as well as the outcome of their cases;

b. ensuring, at least in cases where the victims and their families might be in danger, that they may be informed, if necessary, when the person prosecuted or convicted is released temporarily or definitively;

c. enabling them, in a manner consistent with the procedural rules of internal law, to be heard, to supply evidence and to choose the means of having their views, needs and concerns presented, directly or through an intermediary, and considered;

d. providing them with appropriate support services so that their rights and interests are duly presented and taken into account;

e. protecting their privacy, their identity and their image and by taking measures in accordance with internal law to prevent the public dissemination of any information that could lead to their identification;

f. providing for their safety, as well as that of their families and witnesses on their behalf, from intimidation, retaliation and repeat victimisation;

g. ensuring that contact between victims and perpetrators within court and law enforcement agency premises is avoided, unless the competent authorities establish otherwise in the best interests of the child or when the investigations or proceedings require such contact.

(2) Each Party shall ensure that victims have access, as from their first contact with the competent authorities, to information on relevant judicial and administrative proceedings.

(3) Each Party shall ensure that victims have access, provided free of charge where warranted, to legal aid when it is possible for them to have the status of parties to criminal proceedings.

(4) Each Party shall provide for the possibility for the judicial authorities to appoint a special representative for the victim when, by internal law, he or she may have the status of a party to the criminal proceedings and where the holders of parental responsibility are precluded from representing the child in such proceedings as a result of a conflict of interest between them and

[394] Art. 31(6) Lanzarote Convention.
[395] Art. 35 Lanzarote Convention.
[396] Art. 36(2) Lanzarote Convention.

the victim.

(5) Each Party shall provide, by means of legislative or other measures, in accordance with the conditions provided for by its internal law, the possibility for groups, foundations, associations or governmental or non-governmental organisations, to assist and/or support the victims with their consent during criminal proceedings concerning the offences established in accordance with this Convention.

(6) Each Party shall ensure that the information given to victims in conformity with the provisions of this article is provided in a manner adapted to their age and maturity and in a language that they can understand.

Article 35 Lanzarote Convention – Interviews with the child

(1) Each Party shall take the necessary legislative or other measures to ensure that:

a. interviews with the child take place without unjustified delay after the facts have been reported to the competent authorities;

b. interviews with the child take place, where necessary, in premises designed or adapted for this purpose;

c. interviews with the child are carried out by professionals trained for this purpose;

d. the same persons, if possible and where appropriate, conduct all interviews with the child;

e. the number of interviews is as limited as possible and in so far as strictly necessary for the purpose of criminal proceedings;

f. the child may be accompanied by his or her legal representative or, where appropriate, an adult of his or her choice, unless a reasoned decision has been made to the contrary in respect of that person.

(2) Each Party shall take the necessary legislative or other measures to ensure that all interviews with the victim or, where appropriate, those with a child witness, may be videotaped and that these videotaped interviews may be accepted as evidence during the court proceedings, according to the rules provided by its internal law.

(3) When the age of the victim is uncertain and there are reasons to believe that the victim is a child, the measures established in paragraphs 1 and 2 shall be applied pending verification of his or her age.

Article 36 Lanzarote Convention – Criminal court proceedings

(1) Each Party shall take the necessary legislative or other measures, with due respect for the rules governing the autonomy of legal professions, to ensure that training on children's rights and sexual exploitation and sexual abuse of children is available for the benefit of all persons involved in the proceedings, in particular judges, prosecutors and lawyers.

(2) Each Party shall take the necessary legislative or other measures to ensure, according to the rules provided by its internal law, that:

a. the judge may order the hearing to take place without the presence of the public;

b. the victim may be heard in the courtroom without being present, notably through the use

of appropriate communication technologies.

6.2.3. Guidelines on Child Friendly Justice

As key reference point for how to make a justice system more adaptable to children, the CoE has issued Guidelines on Child-Friendly Justice.[397] These Guidelines also address the position of child victims, particularly when providing evidence in judicial proceedings, and suggest eleven specific measures in line with the Lanzarote Convention for allowing children to give evidence in the most favourable settings and under the most suitable conditions in the light of their age, maturity and level of understanding.[398] To this end, the Guidelines recommend to involve trained professionals[399] and encourage audiovisual statements[400] as well as the opportunity to give evidence in criminal cases without the presence of the alleged perpetrator.[401]

The child-friendly approach promoted in the Guidelines builds on the UN Convention on the Rights of the Child[402] and has the *best interests of the child* as guiding thread.[403] However, the Guidelines are a non-binding instrument even when repeating relevant principles from a binding legal instrument of international law.[404]

6.3. EU Framework

The EU has a solid set of instruments for victim's rights. Complemented by the Compensation Directive and EU rules on European protection orders, the Victims' Rights Directive establishes the right to access information, the right to support and protection, in accordance with victim's individual needs, and a set of procedural rights (section 6.3.1. below). The EU has further adopted instruments that respond to the specific needs of victims of particular crimes like the Anti-Trafficking Directive and the Directive against sexual abuse and sexual exploitation of children (section 6.3.2. below). Because this set of instruments has not yet unfolded its full potential, the European Commission has set out a comprehensive strategy for improving the situation of child victims in the EU (section 6.3.3. below). This comprehensive strategy starts to bear fruits in the Commission's Proposals for a Regulation laying down rules to prevent and combat child sexual abuse (section 6.3.4 below).

[397] CoE, Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice, adopted adopted by the Committee of Ministers of the Council of Europe on 17 November 2010.
[398] CoE, Guidelines on Child-Friendly Justice, at para. 64 – 74.
[399] CoE, Guidelines on Child-Friendly Justice, at para. 64.
[400] CoE, Guidelines on Child-Friendly Justice, at para. 65.
[401] CoE, Guidelines on Child-Friendly Justice, at para. 69.
[402] See section 4.1. above.
[403] E.g.: This guidance has been implemented in Art. 56(2) of the CoE, Convention on preventing and combating violence against women and domestic violence, Convention No. 210, adopted on 11 May 2011, entered in to force on 1 August 2014.
[404] CoE, Guidelines on Child-Friendly Justice, at para. 15. Note for example, how the eleven recommendations in paras. 64. – 74. of the Guidelines mirror the requirements of Art. 31 Lanzarote Convention, as stated in para. 63. of the Guidelines' Explanatory Memorandum.

6.3.1. Victim's Rights Directive

The Victim's Rights Directive 2012/29/EU[405] explicitly recognises the position of child victims and introduces minimum standards for their protection. Art. 1(2) Victim's Rights Directive provides that, when the victim is a child, his or her best interests are a primary consideration and must be assessed on an individual basis. In addition, a *child-sensitive approach* must prevail meaning that the child's age, maturity, views, needs and concerns have to be taken into account, when the child victim (and the child's legal representative) is informed of any measures or rights specifically focused on the child.

During criminal proceedings, child victims have the *right to be heard* and Member States must ensure that child victims can also provide evidence while due account is taken of the child victim's age and maturity.[406] The Member States also have prevent public dissemination of any information leading to the identification of a child victim[407] and are obliged to protect the child victim's privacy, personal integrity and personal data.[408] For the purposes of the Victim's Rights Directive, child victims are presumed to have specific protection needs due to their vulnerability to secondary and repeat victimisation, to intimidation and to retaliation.[409] This leads to protective requirements regarding their interview during a criminal investigation[410] as well as during court proceedings.[411]

Especially for child victims in criminal proceedings, Art. 24 Victim's Rights Directive (a) allows for all interviews with the child victim to be audiovisually recorded and used as evidence, (b) requires the appointment of special representatives, and (c) the right to legal representation in the child victim's own name if there is a conflict of interests between the child victim and the holders of parental responsibility. Last but not least, the Victim's Rights Directive contains various provisions for the protection of victims in general, such as the Right to receive information about their case,[412] and the right to access to victim support services.[413]

Article 1 Victim's Rights Directive – Objectives

1. *The purpose of this Directive is to ensure that victims of crime receive appropriate information, support and protection and are able to participate in criminal proceedings.*

   Member States shall ensure that victims are recognised and treated in a respectful, sensitive, tailored, professional and non-discriminatory manner, in all contacts with victim support or restorative justice services or a competent authority, operating within the context of criminal

[405] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (Victim's Rights Directive), 14 November 2012, Official Journal of the EU, L 315, p. 57.
[406] Art. 10(1) Victim's Rights Directive.
[407] Art. 21(1) Victim's Rights Directive.
[408] Art. 21(2) Victim's Rights Directive.
[409] Art. 22(4) Victim's Rights Directive.
[410] The four requirements set out in Art. 23(2) Victim's Rights Directive not only ensure premises designed for the purpose (a), but also the proper training and the choice of the interviewing professional (b) – (d).
[411] The four requirements set out in Art. 23(3) Victim's Rights Directive aim to avoid (a) visual contact between child victims and offenders, (b) ensure that the child victim may be heard in the courtroom without being physically present, (c) avoid unnecessary questioning concerning the child victim's private life not related to the criminal offence, and (d) the presence of the public during the child victim's hearing.
[412] Art. 6 Victim's Rights Directive.
[413] Art. 8 and 9 Victim's Rights Directive.

proceedings. The rights set out in this Directive shall apply to victims in a non-discriminatory manner, including with respect to their residence status.

2. *Member States shall ensure that in the application of this Directive, where the victim is a child, the child's best interests shall be a primary consideration and shall be assessed on an individual basis. A child-sensitive approach, taking due account of the child's age, maturity, views, needs and concerns, shall prevail. The child and the holder of parental responsibility or other legal representative, if any, shall be informed of any measures or rights specifically focused on the child.*

Article 22 Victim's Rights Directive – Individual assessment of victims to identify specific protection needs

1. *Member States shall ensure that victims receive a timely and individual assessment, in accordance with national procedures, to identify specific protection needs and to determine whether and to what extent they would benefit from special measures in the course of criminal proceedings, as provided for under Articles 23 and 24, due to their particular vulnerability to secondary and repeat victimisation, to intimidation and to retaliation.*
2. *The individual assessment shall, in particular, take into account:*
    (a) the personal characteristics of the victim;
    (b) the type or nature of the crime; and
    (c) the circumstances of the crime.
3. *In the context of the individual assessment, particular attention shall be paid to victims who have suffered considerable harm due to the severity of the crime; victims who have suffered a crime committed with a bias or discriminatory motive which could, in particular, be related to their personal characteristics; victims whose relationship to and dependence on the offender make them particularly vulnerable. In this regard, victims of terrorism, organised crime, human trafficking, gender-based violence, violence in a close relationship, sexual violence, exploitation or hate crime, and victims with disabilities shall be duly considered.*
4. *For the purposes of this Directive, child victims shall be presumed to have specific protection needs due to their vulnerability to secondary and repeat victimisation, to intimidation and to retaliation. To determine whether and to what extent they would benefit from special measures as provided for under Articles 23 and 24, child victims shall be subject to an individual assessment as provided for in paragraph 1 of this Article.*
5. *The extent of the individual assessment may be adapted according to the severity of the crime and the degree of apparent harm suffered by the victim.*
6. *Individual assessments shall be carried out with the close involvement of the victim and shall take into account their wishes including where they do not wish to benefit from special measures as provided for in Articles 23 and 24.*
7. *If the elements that form the basis of the individual assessment have changed significantly, Member States shall ensure that it is updated throughout the criminal proceedings.*

Article 23 Victim's Rights Directive - Right to protection of victims with specific protection needs during criminal proceedings

1. *Without prejudice to the rights of the defence and in accordance with rules of judicial discretion, Member States shall ensure that victims with specific protection needs who benefit from special measures identified as a result of an individual assessment provided for in Article 22(1), may benefit from the measures provided for in paragraphs 2 and 3 of this Article. A special measure envisaged following the individual assessment shall not be made available if operational or practical constraints make this impossible, or where there is a an urgent need to interview the victim and failure to do so could harm the victim or another person or could prejudice the course of the proceedings.*
2. *The following measures shall be available during criminal investigations to victims with specific protection needs identified in accordance with Article 22(1):*
    (a) *interviews with the victim being carried out in premises designed or adapted for that purpose;*
    (b) *interviews with the victim being carried out by or through professionals trained for that purpose;*
    (c) *all interviews with the victim being conducted by the same persons unless this is contrary to the good administration of justice;*
    (d) *all interviews with victims of sexual violence, gender-based violence or violence in close relationships, unless conducted by a prosecutor or a judge, being conducted by a person of the same sex as the victim, if the victim so wishes, provided that the course of the criminal proceedings will not be prejudiced.*
3. *The following measures shall be available for victims with specific protection needs identified in accordance with Article 22(1) during court proceedings:*
    (a) *measures to avoid visual contact between victims and offenders including during the giving of evidence, by appropriate means including the use of communication technology;*
    (b) *measures to ensure that the victim may be heard in the courtroom without being present, in particular through the use of appropriate communication technology;*
    (c) *measures to avoid unnecessary questioning concerning the victim's private life not related to the criminal offence; and*
    (d) *measures allowing a hearing to take place without the presence of the public.*

Article 24 Victim's Rights Directive – Right to protection of child victims during criminal proceedings

1. *In addition to the measures provided for in Article 23, Member States shall ensure that where the victim is a child:*
    (a) *in criminal investigations, all interviews with the child victim may be audiovisually recorded and such recorded interviews may be used as evidence in criminal proceedings;*
    (b) *in criminal investigations and proceedings, in accordance with the role of victims in the relevant criminal justice system, competent authorities appoint a special representative for child victims where, according to national law, the holders of parental responsibility are precluded from representing the child victim as a result of a conflict of interest between them and the child victim, or where the child victim is*

unaccompanied or separated from the family;

(c) where the child victim has the right to a lawyer, he or she has the right to legal advice and representation, in his or her own name, in proceedings where there is, or there could be, a conflict of interest between the child victim and the holders of parental responsibility.

The procedural rules for the audiovisual recordings referred to in point (a) of the first subparagraph and the use thereof shall be determined by national law.

2. Where the age of a victim is uncertain and there are reasons to believe that the victim is a child, the victim shall, for the purposes of this Directive, be presumed to be a child.

The Victim's Rights Directive is complemented by the Victim's Compensation Directive[414] as well as by the EU rules on European protection orders.[415]

6.3.2. Directives on Specific Needs of Child Victims

Before adopting the Victim's Rights Directive, the EU had adopted in 2011 two instruments that respond to the specific needs of child victims of particular crimes: the Anti-Trafficking Directive,[416] and the Directive Against Sexual Abuse and Sexual Exploitation of Children.[417] Both Directives aim to harmonise the preventive criminalisation of their respective crimes and to establish a set of child victim's rights which especially relevant in the context of CSE and CSEM material.

- **Anti-Trafficking Directive**

The Anti-Trafficking Directive 2011/36/EU establishes the rule that a child victim of trafficking in human beings is provided with the assistance, support and protection serving the child's best interests.[418] Independently of any criminal investigation or court proceeding, the assistance and support measures have to cater to the individual child victim's physical and psycho-social recovery in the short and long term.[419]

For criminal investigations and proceedings, child victims not only have to be appointed a representative,[420]

[414] Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims, Official Journal of the EU, 6 August 2004, L 261, p. 15.
[415] Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order and Regulation (EU) No 606/2013 of the European Parliament and of the Council of 12 June 2013 on mutual recognition of protection measures in civil matters.
[416] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, Official Journal of the EU, 15 April 2011, L 101, p. 1.
[417] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Official Journal of the EU, 17 December 2011, L 335, p. 1.
[418] Art. 13(1) Anti-Trafficking Directive.
[419] Art. 14(1) Anti-Trafficking Directive.
[420] Art. 15(1) Anti-Trafficking Directive.

but also have undelayed access to free legal counselling and to free legal representation, including for the purpose of claiming compensation,[421] unless they have sufficient financial resources.[422] Member States have to take the necessary measures to ensure that any interview of the child victim in the course of a criminal investigation and proceeding meets the procedural requirements set out in Art. 15(3), (4) and (5) Anti-Trafficking Directive which overlap and partially supplement the procedural requirements established in Art. 23(2) and (3) Victim's Rights Directive.

Article 13 Anti-Trafficking Directive – General provisions on assistance, support and protection measures for child victims of trafficking in human beings

1. *Child victims of trafficking in human beings shall be provided with assistance, support and protection. In the application of this Directive the child's best interests shall be a primary consideration.*
2. *Member States shall ensure that, where the age of a person subject to trafficking in human beings is uncertain and there are reasons to believe that the person is a child, that person is presumed to be a child in order to receive immediate access to assistance, support and protection in accordance with Articles 14 and 15.*

Article 14 Anti-Trafficking Directive – Assistance and support to child victims

1. *Member States shall take the necessary measures to ensure that the specific actions to assist and support child victims of trafficking in human beings, in the short and long term, in their physical and psycho-social recovery, are undertaken following an individual assessment of the special circumstances of each particular child victim, taking due account of the child's views, needs and concerns with a view to finding a durable solution for the child. Within a reasonable time, Member States shall provide access to education for child victims and the children of victims who are given assistance and support in accordance with Article 11, in accordance with their national law.*
2. *Members States shall appoint a guardian or a representative for a child victim of trafficking in human beings from the moment the child is identified by the authorities where, by national law, the holders of parental responsibility are, as a result of a conflict of interest between them and the child victim, precluded from ensuring the child's best interest and/or from representing the child.*
3. *Member States shall take measures, where appropriate and possible, to provide assistance and support to the family of a child victim of trafficking in human beings when the family is in the territory of the Member States. In particular, Member States shall, where appropriate and possible, apply Article 4 of Framework Decision 2001/220/JHA to the family.*
4. *This Article shall apply without prejudice to Article 11.*

Article 15 Anti-Trafficking Directive – Protection of child victims of trafficking in human beings in

[421] Art. 17 Anti-Trafficking Directive requires Member States to provide (child) victims with access to existing schemes of compensation to victims of violent crimes of intent.
[422] Art. 15(2) Anti-Trafficking Directive.

criminal investigations and proceedings

1. *Member States shall take the necessary measures to ensure that in criminal investigations and proceedings, in accordance with the role of victims in the relevant justice system, competent authorities appoint a representative for a child victim of trafficking in human beings where, by national law, the holders of parental responsibility are precluded from representing the child as a result of a conflict of interest between them and the child victim.*
2. *Member States shall, in accordance with the role of victims in the relevant justice system, ensure that child victims have access without delay to free legal counselling and to free legal representation, including for the purpose of claiming compensation, unless they have sufficient financial resources.*
3. *Without prejudice to the rights of the defence, Member States shall take the necessary measures to ensure that in criminal investigations and proceedings in respect of any of the offences referred to in Articles 2 and 3:*
    (a) *interviews with the child victim take place without unjustified delay after the facts have been reported to the competent authorities;*
    (b) *interviews with the child victim take place, where necessary, in premises designed or adapted for that purpose;*
    (c) *interviews with the child victim are carried out, where necessary, by or through professionals trained for that purpose;*
    (d) *the same persons, if possible and where appropriate, conduct all the interviews with the child victim;*
    (e) *the number of interviews is as limited as possible and interviews are carried out only where strictly necessary for the purposes of criminal investigations and proceedings;*
    (f) *the child victim may be accompanied by a representative or, where appropriate, an adult of the child's choice, unless a reasoned decision has been made to the contrary in respect of that person.*
4. *Member States shall take the necessary measures to ensure that in criminal investigations of any of the offences referred to in Articles 2 and 3 all interviews with a child victim or, where appropriate, with a child witness, may be video recorded and that such video recorded interviews may be used as evidence in criminal court proceedings, in accordance with the rules under their national law.*
5. *Member States shall take the necessary measures to ensure that in criminal court proceedings relating to any of the offences referred to in Articles 2 and 3, it may be ordered that:*
    (a) *the hearing take place without the presence of the public; and*
    (b) *the child victim be heard in the courtroom without being present, in particular, through the use of appropriate communication technologies.*
6. *This Article shall apply without prejudice to Article 12.*

- **Directive Against Sexual Abuse and Sexual Exploitation of Children**

The main focus of the Directive Against Sexual Abuse and Sexual Exploitation of Children 2011/93/EU is to establishes minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children, "child pornography" and solicitation of children for sexual purposes. However, Directive 2011/93/EU also introduces provisions to strengthen the protection of the victims thereof:[423]

While child victims are neither to be prosecuted nor to be imposed penalties for their involvement in criminal activities, which they have been compelled to commit as a direct consequence of being subjected offences concerning their sexual exploitation or "child pornography",[424] establishes the rule that a child victim of these offences is provided with the assistance, support and protection serving the child's best interests.[425] This assistance and support has to be provided before, during and for an appropriate period of time after the conclusion of criminal proceedings in order to enable them to exercise the rights.[426]

For criminal investigations and proceedings, child victims not only have to be appointed a representative,[427] but also have undelayed access to free legal counselling and to free legal representation, including for the purpose of claiming compensation,[428] unless they have sufficient financial resources.[429] Member States have to take the necessary measures to ensure that any interview of the child victim in the course of a criminal investigation and proceeding meets the procedural requirements set out in Art. 20(3), (4) and (5) Directive 2011/93/EU which are identical to the procedural requirements established in Art. 15 Anti-Trafficking Directive. These procedural requirements overlap and partially supplement the procedural requirements established in Art. 23(2) and (3) Victim's Rights Directive which was adopted a year later.

Article 18 Directive 2011/93/EU – General provisions on assistance, support and protection measures for child victims

1. *Child victims of the offences referred to in Articles 3 to 7 shall be provided assistance, support and protection in accordance with Articles 19 and 20, taking into account the best interests of the child.*
2. *Member States shall take the necessary measures to ensure that a child is provided with assistance and support as soon as the competent authorities have a reasonable-grounds indication for believing that a child might have been subject to any of the offences referred to in Articles 3 to 7.*
3. *Member States shall ensure that, where the age of a person subject to any of the offences referred to in Articles 3 to 7 is uncertain and there are reasons to believe that the person is a child, that person is presumed to be a child in order to receive immediate access to assistance, support and protection in accordance with Articles 19 and 20.*

[423] Art. 1 Directive 2011/93/EU.
[424] Art. 14 Directive 2011/93/EU referring to Art. 4(2), (3), (5) and (6) regarding sexual exploitation and to Art. 5(6) regarding "child pornography".
[425] Art. 18(1) Directive 2011/93/EU.
[426] Art. 19(1) Directive 2011/93/EU.
[427] Art. 20(1) Directive 2011/93/EU.
[428] The right to compensation emanates from Framework Decision 2001/220/JHA which establishes a set of victims' rights in criminal proceedings, see: Recital 32 Directive 2011/93/EU.
[429] Art. 20(2) Directive 2011/93/EU.

Article 19 Directive 2011/93/EU – Assistance and support to victims

1. *Member States shall take the necessary measures to ensure that assistance and support are provided to victims before, during and for an appropriate period of time after the conclusion of criminal proceedings in order to enable them to exercise the rights set out in Framework Decision 2001/220/JHA, and in this Directive. Member States shall, in particular, take the necessary steps to ensure protection for children who report cases of abuse within their family.*
2. *Member States shall take the necessary measures to ensure that assistance and support for a child victim are not made conditional on the child victim's willingness to cooperate in the criminal investigation, prosecution or trial.*
3. *Member States shall take the necessary measures to ensure that the specific actions to assist and support child victims in enjoying their rights under this Directive, are undertaken following an individual assessment of the special circumstances of each particular child victim, taking due account of the child's views, needs and concerns.*
4. *Child victims of any of the offences referred to in Articles 3 to 7 shall be considered as particularly vulnerable victims pursuant to Article 2(2), Article 8(4) and Article 14(1) of Framework Decision 2001/220/JHA.*
5. *Member States shall take measures, where appropriate and possible, to provide assistance and support to the family of the child victim in enjoying the rights under this Directive when the family is in the territory of the Member States. In particular, Member States shall, where appropriate and possible, apply Article 4 of Framework Decision 2001/220/JHA to the family of the child victim.*

Article 20 Directive 2011/93/EU – Protection of child victims in criminal investigations and proceedings

1. *Member States shall take the necessary measures to ensure that in criminal investigations and proceedings, in accordance with the role of victims in the relevant justice system, competent authorities appoint a special representative for the child victim where, under national law, the holders of parental responsibility are precluded from representing the child as a result of a conflict of interest between them and the child victim, or where the child is unaccompanied or separated from the family.*
2. *Member States shall ensure that child victims have, without delay, access to legal counselling and, in accordance with the role of victims in the relevant justice system, to legal representation, including for the purpose of claiming compensation. Legal counselling and legal representation shall be free of charge where the victim does not have sufficient financial resources.*
3. *Without prejudice to the rights of the defence, Member States shall take the necessary measures to ensure that in criminal investigations relating to any of the offences referred to in Articles 3 to 7:*
    - *(a) interviews with the child victim take place without unjustified delay after the facts have been reported to the competent authorities;*
    - *(b) interviews with the child victim take place, where necessary, in premises designed or adapted for this purpose;*
    - *(c) interviews with the child victim are carried out by or through professionals trained for*

this purpose;

(d) the same persons, if possible and where appropriate, conduct all interviews with the child victim;

(e) the number of interviews is as limited as possible and interviews are carried out only where strictly necessary for the purpose of criminal investigations and proceedings;

(f) the child victim may be accompanied by his or her legal representative or, where appropriate, by an adult of his or her choice, unless a reasoned decision has been made to the contrary in respect of that person.

4. *Member States shall take the necessary measures to ensure that in criminal investigations of any of the offences referred to in Articles 3 to 7 all interviews with the child victim or, where appropriate, with a child witness, may be audio-visually recorded and that such audio-visually recorded interviews may be used as evidence in criminal court proceedings, in accordance with the rules under their national law.*

5. *Member States shall take the necessary measures to ensure that in criminal court proceedings relating to any of the offences referred to in Articles 3 to 7, that it may be ordered that:*

(a) the hearing take place without the presence of the public;

(b) the child victim be heard in the courtroom without being present, in particular through the use of appropriate communication technologies.

6. *Member States shall take the necessary measures, where in the interest of child victims and taking into account other overriding interests, to protect the privacy, identity and image of child victims, and to prevent the public dissemination of any information that could lead to their identification.*

6.3.3. EU Strategy on Victims' Rights (2020–2025)

In 2020, the Report on the implementation of the Victim's Rights Directive[430] and the Report on the implementation of the Directive on European protection order[431] revealed significant shortcomings in the Member States' implementation of harmonised victims' rights. These shortcomings were reminiscent of the previous two Reports on the implementation of the Child Sexual Abuse Directive[432] and the Report on the

[430] Report from the Commission to the European Parliament and the Council on the implementation of the Victims' Rights Directive, COM(2020)188 final, 11 May 2020, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:188:FIN.

[431] Report from the Commission to the European Parliament and the Council on the implementation of Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order, COM(2020)187final, 11 May 2020, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:187:FIN

[432] Two reports: Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, COM/2016/0871 final, 16 December 2016, available at: https://eur-lex.europa.eu/legal-

implementation of the Anti-Trafficking Directive[433], both of which had revealed essential shortcomings as well. In the light of all these shortcomings and because the lockdown of society during the COVID-19 pandemic had led to a rise in domestic violence, child sexual abuse and cybercrime, the European Commission issued a first EU Strategy on victims' rights in June 2020 in order to strengthen the framework for support and protection of victims and ensure it is resilient in crisis situations.[434]

Summarising the bigger picture revealed by the implementation Reports mentioned above, the Commission points out that victims' difficulties in accessing justice are mainly due to lack of information, insufficient support and protection. Victims are often exposed to secondary victimisation during criminal proceedings and when claiming compensation. Those who become victims of crime when travelling abroad find it even more difficult to access justice and compensation. For the most vulnerable victims including child victims it remains particularly challenging to go through criminal proceedings and to deal with the aftermath of crime.[435]

In order to improve the situation for victims, it is crucial that all Member States fully implement and apply the agreed minimum standards described in this section 6.3. Therefore, the Commission will focus on ensuring the correct implementation of these existing EU rules on victims' rights in practice.[436] Based on a two-strand approach, empowering victims of crime and working together for victims' rights, the Commission elaborates five key priorities for the next five years: (i) effective communication with victims and a safe environment for victims to report crime;[437] (ii) improving support and protection to the most vulnerable victims;[438] (iii) facilitating victims' access to compensation;[439] (iv) strengthening cooperation and coordination among all

content/EN/TXT/?uri=CELEX%3A52016DC0871; Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, COM/2016/0872 final, 16 December 2016, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2016:872:FIN.

[433] Report from the Commission to the European Parliament and the Council assessing the extent to which Member States have taken the necessary measures in order to comply with Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims in accordance with Article 23 (1), COM(2016) 722 final, 2 December 2016, available at: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/report_on_member_states_compliance_with_directive_2011-36_en.pdf.

[434] Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions on EU Strategy on victims' rights (2020-2025), COM(2020) 258 final, 24 June 2020, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0258&from=EN.

[435] Commission, Communication on EU Strategy on victims' rights (2020-2025), COM(2020) 258 final, 24 June 2020, p. 2.

[436] Commission, Communication on EU Strategy on victims' rights (2020-2025), COM(2020) 258 final, 24 June 2020, p. 3.

[437] Commission, Communication on EU Strategy on victims' rights (2020-2025), COM(2020) 258 final, 24 June 2020, p. 4 et seq.

[438] Commission, Communication on EU Strategy on victims' rights (2020-2025), COM(2020) 258 final, 24 June 2020, p. 8 et seq.

[439] Commission, Communication on EU Strategy on victims' rights (2020-2025), COM(2020) 258 final, 24 June 2020, p. 16 et seq.

relevant actors;[440] and (v) strengthening the international dimension of victims' rights.[441]

Update for Legal Report v2:

6.3.4. Victims' Rights in Draft Regulation Against Online CSA

In line with its two-strand approach of empowering victims of crime, on the one hand, and working together for victims' rights, on the other, the Commission has included strong victims' rights in its Proposal for a Regulation laying down rules to prevent and combat child sexual abuse[442] (Draft Regulation Against Online CSA). The harmonised legal framework proposed in the Draft Regulation Against Online CSA is described in more detail in chapter 4. above. For this chapter's focus on victims' rights, it suffices to focus solely on the two specific rights for victims established in Chapter II of the Draft Regulation Against Online CSA.

First of all, victims of CSA are granted the right to receive from the EU Centre information on any report of known CSA material depicting them, Art. 20(1) Draft Regulation Against Online CSA. Upon request via the national Coordinating Authority of their place of residence, the EU Centre must provide information about:[443] (a) the identification of the provider that submitted the report; (b) the date of the report; (c) whether the EU Centre forwarded the report to Europol and/or which national LEAs; and (d) whether the provider reported has removed or disabled access to the CSA material[444].

In addition, victims of CSA are granted the right to assistance and to support for the removal of CSA material depicting them, Art. 21 Draft Regulation Against Online CSA. Hosting providers have to provide "reasonable assistance" to victims seeking to have known CSA material depicting them either removed or access to thereto disabled.[445] Upon their request via the national Coordinating Authority of their place of residence, victims also have the right to receive support from the EU Centre when they seek to have a hosting provider remove or disable access to known CSA material depicting them.[446] Because children with disabilities face a significantly higher risk of experiencing sexual violence,[447] victims with disabilities are granted the right to ask and receive any information relating to such support in a manner accessible to them.[448] One advantage of receiving support from the EU Centre is that the victim's request is communicated between the national Coordinating

[440] Commission, Communication on EU Strategy on victims' rights (2020-2025), COM(2020) 258 final, 24 June 2020, p. 19 et seq.
[441] Commission, Communication on EU Strategy on victims' rights (2020-2025), COM(2020) 258 final, 24 June 2020, p. 21 et seq.
[442] Commission, Proposal for a Regulation of the European Parliament and the Council laying down rules to prevent and combat child sexual abuse, COM (2021) 209 final, 2022/0155 (COD), 11 May 2022, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209&from=EN.
[443] Art. 20(4) Draft Regulation Against Online CSA.
[444] This information is a mandatory requirement in any report of potential CSA material, Art. 13(1)(i) Draft Regulation Against Online CSA.
[445] Art. 21(1) Draft Regulation Against Online CSA.
[446] Art. 21(2) subparagraph 1 sentence 1 Draft Regulation Against Online CSA.
[447] Commission, Draft Regulation Against Online CSA, COM (2021) 209 final, 11 May 2022, Explanatory Memorandum, p. 1 referring to the comprehensive information on "Children with Disabilities" provided by the UN Special Representative of the Secretary-General on Violence Against Children at: https://violenceagainstchildren.un.org/content/children-disabilities.
[448] Art. 21(2) subparagraph 1 sentence 2 Draft Regulation Against Online CSA.

Authority, the EU Centre and the respective hosting provider through the secure information sharing system established by the EU Centre pursuant Art. 39(2) Draft Regulation Against Online CSA.[449] Another advantage of the right to receive support is that the EU Centre is effectively intended to achieve the removal for the victim because, in addition to (a) requesting the respective hosting provider's assistance, the EU Centre's support also has to include:[450] (b) verifying whether the provider removed or disabled access to the CSA material, including by conducting the searches[451]; (c) notifying the known CSA material depicting the victim to the provider and requesting removal or disabling of access; and even (d) informing the competent Coordinating Authority of that known CSA material on the hosting provider's service, with a view to the issuance of a removal order pursuant to Art. 14 Draft Regulation Against Online CSA.

[449] Art. 21(2) subparagraph 2 Draft Regulation Against Online CSA.
[450] Art. 21(4) Draft Regulation Against Online CSA.
[451] Upon request for support by a victim, the EU Centre is granted the power to conduct searches on hosting services in order to verify whether the hosting provider has removed the known CSA material depicting the victim, Art. 49(1)(a) Draft Regulation Against Online CSA.

7. Data Protection

This chapter provides an overview of the relevant legal framework for data protection at European level for two phases regarding the GRACE project: First there is the *research phase* during which the GRACE tools and platform are developed as prototype (section 6.1. below) and second there is the *after-roll-out phase* when the GRACE tools and platform are potentially put to use by LEAs in their fight against CSEM (section 6.2. below). For both phases, there are in Europe two separate and overlapping legal regimes governing the protection of personal data emanating from the right to respect for private and family life enshrined in the European Convention on Human Rights (ECHR), on the one side, and the Charter of Fundamental Rights of the European Union (Charter of Fundamental Rights), on the other:

- In the framework established by the Council of Europe (CoE), the participating states (Parties) base their guarantee of human rights on the European Convention for the Protection of Human Rights and Fundamental Freedoms[452] better known as the European Convention on Human Rights (ECHR). Because the ECHR was declared considering the Universal Declaration of Human Rights (UDHR)[453], the ECHR comprises much the same guarantees of fundamental rights and freedoms as the UDHR.
- In the framework provided by the European Union (EU), the Charter of Fundamental Rights of the European Union (2000) has been established for the protection of human rights. Concerning the protection of privacy, the Charter of Fundamental Rights comprises not only the right to respect for private and family life[454] but also the right to protection of personal data[455] implying a more coherent approach. The guarantees of the Charter of Fundamental Rights also include the freedom of expression and information[456], freedom of assembly and of association[457] as well as the right to a fair trial[458] and the presumption of innocence[459].

7.1. Research Phase: Development of GRACE Prototypes

The vision of the GRACE project is to develop advanced high-level digital and analytical tools made available to LEAs via a Federated Platform which transforms their investigative capabilities into a synchronised and impactful response to the immense influx of CSEM reports. At the moment, LEAs in some EU Member States receive referrals by the NCMEC and NCECC directly (e.g., Austria, France, Germany, Ireland, Italy, Lithuania, Netherlands, Portugal and Spain) whereas LEAs in other EU Member States receive these referrals by using Europol as the catalyst (e.g., Belgium, Cyprus, Poland and Romania).

---

[452] Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols Nos. 11 and 14 and supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13), 4 December 1950.

[453] United Nations, General Assembly, Universal Declaration of Human Rights (UDHR) Resolution 217 A, A/RES/3/217 A, 10 December 1948.

[454] Art. 7 Charter of Fundamental Rights.

[455] Art. 8 Charter of Fundamental Rights.

[456] Art. 10 Charter of Fundamental Rights.

[457] Art. 11 Charter of Fundamental Rights.

[458] Art. 47 Charter of Fundamental Rights.

[459] Art. 48 Charter of Fundamental Rights.

For tackling the influx of CSEM reports, the GRACE project develops Big Data solutions for data ETL[460] which will not only standardise the management of CSEM reports, but also avoid duplicate processing and enhance collaboration amongst national LEAs within the EU. The data of each CSEM report will be analysed in terms of visual, audio and text information using AI technologies to produce structured and validated information from the CSEM report's content. For this purpose, GRACE will develop novel forensic analysis tools for (i) CSEM-specific content analysis and classification, (ii) content-based geo-localisation, (iii) the creation of evidence graphs to connect cases, (iv) case prioritisation techniques and (v) predictive analysis of trends in CSE offenders' tactics. For the operational coordination of LEAs in all Member States, a Federated (Machine) Learning platform will be developed and established which will exploit available infrastructure as well as the metadata of any CSEM content distributed across the entire EU.

7.1.1. CoE Framework for Data Protection in Research

In the framework established by the Council of Europe (CoE), the ECHR is designed for the protection of an individual against activities of the state and does not provide privileges for research activities.

The right to personal data protection forms part of the rights protected under Art. 8 ECHR, which guarantees the right to respect for private and family life, home and correspondence, and lays down the conditions under which restrictions of this right are permitted. The respect for private life is not an absolute right, as the exercise of the right to privacy could compromise other rights.

Rather, scientific research as carried out in the course of the GRACE project falls within the scope of the 1981 Convention for the Protection of Individuals with Regard to the Processing of Personal Data, better known as Convention 108. Convention 108 applies to all data processing carried out by both the private and public sectors, including data processing by the judiciary and law enforcement authorities. It protects individuals against abuses that may accompany the processing of personal data, and seeks, at the same time, to regulate the trans-border flows of personal data. As regards the processing of personal data, the principles laid down in the convention concern, in particular, fair and lawful collection and automatic processing of data, for specified legitimate purposes. This means that the data should not be used for ends incompatible with these purposes and should be kept for no longer than is necessary. They also concern the quality of the data, in particular that they must be adequate, relevant and not excessive (proportionality), as well as accurate.

Convention 108 is binding for states that have ratified it and all EU Member States have ratified Convention 108. It is not subject to the judicial supervision of the ECtHR, but has been taken into consideration in the case law of the ECtHR within the context of Art. 8 ECHR. Over the years, the ECtHR has ruled that personal data protection is an important part of the right to respect for private life (Art. 8 ECHR), and has been guided by the principles of Convention 108 in determining whether or not there has been an interference with this fundamental right.[461]

Convention 108 has been modernised into Convention 108+ in 2018 to align with the EU's General Data

[460] ETL = Extract, Transform, Load; referring to the general procedure of copying data from one or more sources into a destination system which represents the data differently from the source(s) or in a different context than the source(s), see: https://en.wikipedia.org/wiki/Extract,_transform,_load.
[461] See for example: ECtHR, decision of 25 February 1997, *Z v. Finland*, Application No. 22009/93, at para. 95.

Protection Regulation.[462] Convention 108+ has been opened for signature on 10 October 2018 for the Contracting States to Convention 108 and will enter into force either when all Parties to Convention 108 have ratified the amending Protocol or on 11 October 2023 if there are 38 Parties to the amending Protocol by then.[463]

For the legitimacy of personal data processing, Art. 5 Convention 108+ requires the processing of personal data to be lawful (Art. 5(3) Convention 108+) as well as fair and transparent (Art. 5(4)(a) Convention 108+) for the data subject. In addition, Art. 5(4)(b) Convention 108+ establishes the concept of compatible use according to which data collected for explicit, specified and legitimate purposes may not be processed in a way incompatible with those purposes.[464] However "further processing of personal data" for scientific research purposes is *a priori* considered as compatible provided that the operations, in principle, exclude any use of the information obtained for decisions or measures concerning a particular individual[465] and that other safeguards exist, Art. 5(4)(b) Convention 108+. The Explanatory Report to Art. 5 Convention 108+ mentions explicitly as examples for suitable safeguards in this respect:

- the anonymisation or pseudonymisation of data, except if retention of the identifiable form is necessary;
- rules of professional secrecy;
- provisions governing restricted access and communication of data for the scientific purposes; and
- other technical and organisational data-security measures.[466]

Because the GRACE project has already established such safeguards, its processing of personal data would seem to be legitimate and in accordance with Art. 5 Convention 108+. However, Convention 108+ has yet to enter into force. Therefore, the CoE framework for the legitimacy of processing data for scientific research purposes is set by Convention 108 (as amended in 1999) without the modernizing amendments adopted in 2018. According to Art. 9(3) Convention 108, the exercise of the data subjects' rights may be restricted by law with regard to data processing operations for scientific research purposes "when there is obviously no risk of an infringement of the privacy of the data subjects".[467]

Interference with this right by a public authority is prohibited, except where the interference is in accordance with the law, pursues important and legitimate public interests and is necessary in a democratic society.

Article 8 Convention 108 – Additional safeguards for the data subject

[462] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.
[463] See Chart of signatures and ratifications of Treaty 223 available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures.
[464] This seems an equivalent to principle of purpose limitation enshrined in Art. 5(1)(b) GDPR.
[465] Explanatory Report to Convention 108+, p. 21 at para. 50, available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
[466] Explanatory Report to Convention 108+, p. 21 at para. 50, available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
[467] Explanatory Report to Convention 108, p. 11 at para. 59, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434.

Any person shall be enabled:

a. *to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;*

b. *to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;*

c. *to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;*

d. *to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.*

Article 9 Convention 108 – Exceptions and restrictions

1. *No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.*
2. *Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:*

   (a) *protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;*

   (b) *protecting the data subject or the rights and freedoms of others.*
3. *Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.*

Article 5 Convention 108+ – Legitimacy of data processing and quality of data

1. *Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.*
2. *Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.*
3. *Personal data undergoing processing shall be processed lawfully.*
4. *Personal data undergoing processing shall be:*

   a. *processed fairly and in a transparent manner;*

   b. *collected for explicit, specified and legitimate purposes and not processed in a way*

incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes;

c. *adequate, relevant and not excessive in relation to the purposes for which they are processed;*

d. *accurate and, where necessary, kept up to date;*

e. *preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.*

7.1.2. EU Framework for Data Protection in Research

In the framework provided by the European Union (EU), the data protection standards are based on Convention 108. The fundamental right to protection of personal data enshrined in Art. 8 Charter of Fundamental Rights and codified in Art. 16 TFEU[468]. Granting the EU competence to legislate on data protection matters, Art. 16 TFEU provides the legal basis for a modern, comprehensive approach to data protection, which covers all matters of EU competence, including police and judicial cooperation in criminal matters.

The principal legal instrument on the guarantee of data protection in the EU is the General Data Protection Regulation[469] (GDPR)[470] which not only requires an explicit legal basis but also proportionality for each individual encroachment. The GDPR establishes a legal regime particularly favourable for research. The legal regime of the GDPR distinguishes between historical and scientific research. These research purposes are pooled in Art. 89 GDPR with two neighbouring scopes namely archiving in the public interest and statistics. Because there are normative differences between these four processing purposes, it is helpful to identify the purposes relevant for the GRACE project.

The four processing purposes are explained only in the Recitals of the GDPR. While historical research purposes include historical research and research for genealogical purposes,[471] archiving in the public interest

[468] Treaty of the Functioning of the European Union (TFEU), 26 October 2012, Official Journal of the EU, C 326/47, p. 55.

[469] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the EU, L 119/1.

[470] The GDPR succeeded Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), Official Journal 1995, L 281. From 1995 to May 2018, the Data Protection Directive reflected the data protection principles already contained in national laws and in Convention 108, while often expanding them. Drawing on Art. 11 Convention 108, the Data Protection Directive introduced independent supervision as an instrument for improving compliance with data protection rules and this feature was incorporated into the CoE framework in 2001 by the Additional Protocol to Convention 108 illustrating the mutual interaction and positive influence between the CoE and the EU framework.

[471] Recital 160 sentence 2 GDPR.

refers to services by public or private bodies which have a legal obligation to maintain records of enduring value for general public interest.[472] Neither of these two processing purposes seems relevant for activities carried out in the course of the GRACE project, leaving processing for scientific research and statistical purposes:

7.1.2.1. Scientific Research and Statistics as Processing Purposes

The GDPR does not provide a definition of scientific research but requires a broad interpretation of this concept and lists several examples including "technological development and demonstration, fundamental research, applied research and privately funded research".[473] Scientific research is, therefore, any activity aimed at generating new knowledge and advancing the state-of-the-art in a given field which also includes activities for profit like e.g. experimental development carried out by a company to improve or offer new services.[474]

The technological development of the GRACE tools and platform falls squarely under this definition. The novel forensic analysis tools for (i) CSEM-specific content analysis and classification, (ii) content-based geo-localisation, (iii) the creation of evidence graphs to connect cases, (iv) case prioritisation techniques and (v) predictive analysis of trends in CSE offenders' tactics, will all improve the state-of-the-art regarding the analysis of CSEM reports. Once these GRACE tools and the Federated (Machine) Learning platform have been developed, it seems more than unlikely that the GRACE platform's continuous exploitation of the CSEM report's metadata for trends in CSE offenders' tactics will continue to fall under the GDPR's concept of scientific research.

Statistical purposes are defined as any processing of personal data necessary for statistical surveys or for the production of statistical results.[475] The data generated through the statistical process has to be aggregated, meaning that the result cannot consist of data referable to a particular individual and the statistical results may be re-used for different purposes, including for further processing for scientific purposes.[476] Two distinct features characterise statistical processing:

(i) statistical processing aims at creating basic knowledge because it is not an end to itself and usually serves other purposes including scientific research,[477] and

[472] Recital 158 sentence 2 GDPR.
[473] Art. 159 sentence 2 GDPR.
[474] Ducato, "Data Protection, Scientific Research, and the Role of Information", Computer Law & Security Review 37 (2020) 105412, p. 3, pointing out that the explicit reference to Art. 179(1) TFEU in Recital 159 sentence 3 GDRP confirms the importance of the private and industrial component in the context of scientific and technological development within the European Research Area.
[475] Recital 162 sentence 3 GDPR.
[476] Recital 162 sentence 4 and 5 GDPR.
[477] CoE, Explanatory Memorandum – Recommendation No.R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997, at paras. 11. and 11.c).

(ii) statistical purposes exclude personalised impacts on individuals[478] and any individual data collected for statistical purposes, that is to say in order to visualise mass phenomena, are only raw material intended ultimately to lose their individuality in a statistical result.[479]

Statistics shares the first feature with scientific research and the basic knowledge generated by the analysis of data about a collective phenomenon in a given reference group can be further used for other purposes, as results of scientific research can later be exploited in applied science or technological development.[480] In contrast, the second feature appears to offer a criterion for distinguishing statistics form scientific research by requiring that neither the result (*output data*) nor the personal data used to generate that result (*input data*) are used to support measures or decisions concerning an individual.[481] As a consequence, when an entity uses personal data of individuals to develop a predictive model able to measure particular phenomena among these individuals, such data processing would serve statistical purposes within the meaning of Art. 89 GDPR and, therefore, be privileged.[482] Unfortunately however, the GDPR remains silent about the potential impact of scientific research results on individuals and leaves it for the Member States to delineate the exact boundaries of the concept of scientific research in this respect, so that Member States' national law may or may not require the exclusion of personalised measures or decisions about an individual.[483] This allows to conclude that the data protection privileges set out in Art. 89 GDPR apply when statistical or scientific research processes are run to generate new knowledge without any specific impact on an individual. Consequently, the privileged data protection regime laid down in Art. 89 GDPR will also apply to the GRACE platform's continuous exploitation of the CSEM report's metadata in any case as long as the predictive analysis of trends in CSE offenders' tactics does not lead to personalised measures or decisions about specific individuals. As soon as the elicitation of trends in CSE crimes would be combined with individualised decisions by the GRACE system, then the privileged data protection regime according to Art. 89 GDPR will not apply.

7.1.2.2. The Privileged Data Protection Regime under Art. 89 GDPR

The privileged data protection regime set out in Art. 89 GDPR provides a specific balance between the fundamental rights of individuals, the freedom to conduct a business and the legitimate expectations of

[478] CoE, Explanatory Memorandum – Recommendation No.R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997, at paras. 3., 9., 14.b), 27. and 58.
[479] CoE, Explanatory Memorandum – Recommendation No.R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997, at paras. 57.a) and 57.b).
[480] Ducato, "Data Protection, Scientific Research, and the Role of Information", Computer Law & Security Review 37 (2020) 105412, p. 4.
[481] Recital 162 sentence 5 GDPR.
[482] Ducato, "Data Protection, Scientific Research, and the Role of Information", Computer Law & Security Review 37 (2020) 105412, p. 4.
[483] Ducato, "Data Protection, Scientific Research, and the Role of Information", Computer Law & Security Review 37 (2020) 105412, p. 4, stating that processing for statistical or for scientific research purposes both require the exclusion of personalised impacts on individuals e.g. in Cyprus, France, Italy, Luxembourg, Sweden and the UK. However, this requirement does not apply to processing for scientific research purposes e.g. in Germany.

society for an increase of knowledge.[484] Provided that appropriate safeguards for the rights and freedoms of data subjects are in place,[485] the privileged data processing benefits not only from *exceptions* to the principles of purpose limitation[486] and storage limitation[487] as well as to the strict regime for processing special categories of personal data[488], but also from *derogations* to the exercising of the data subject's right to be provided information,[489] right of access,[490] right to rectification,[491] right to erasure,[492] right to restriction of processing,[493] and right to object.[494]

7.1.2.2.1. Exceptions to Fundamental Data Protection Principles

Concerning the principle of *purpose limitation*, the GDPR establishes a presumption of compatibility between (secondary) processing for the purposes privileged under Art. 89 GDPR and the original purpose of collection.[495] Regarding the principle of *storage limitation*, the data processed for the purposes privileged in Art. 89 GDPR may be kept in a form which allows identification of individuals even beyond the period strictly necessary for the achievement of their collection's original purpose.[496] While this exception to the principle of storage limitation works in favour of the verification of research results, it also appears to be prone to abuse because the intention seems to have been to dissuade unlimited storage even in the privileged data protection regime so that the privileged purposes may not be serve as pretext for longer storage for other purposes.[497]

The exception regarding processing of special categories of personal data is more complex. Art. 9(2)(j) GDPR provides that (i) national or Union law may authorise the processing of sensitive data provided that the processing is (ii) necessary for the achievement of the purposes privileged in Art. 89 GDPR and (iii) proportionate to the scope pursued. This provision also explicitly refers to the "essence of the right to data protection" requiring that it is respected. This reference might include the core principles of fairness, purpose limitation and lawfulness as well as the right of access and rectification as enshrined in Art. 8(2) Charter of Fundamental Rights, or the principles of purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality as well as accountability as enshrined in Art. 5 GDPR, or both. However, the appropriate and specific measures to protect the fundamental rights and the interests of the individuals seem to be needed in addition to the safeguard already required by Art. 89(1) GDPR for the processing of personal data.[498]

---

[484] Recitals 4 and 113 sentence 4 GDPR.
[485] See Art. 25 and 32 GDPR.
[486] Art. 5(b) GDPR.
[487] Art. 5(e) GDPR.
[488] Art. 9(2)(j) GDPR.
[489] Art. 14(5)(b) GDPR.
[490] Art. 15, 89(2) GDPR.
[491] Art. 16, 89(2) GDPR.
[492] Art. 17(3)(d) GDPR
[493] Art. 18, 89(2) GDPR.
[494] Art. 21(6), 89(2) GDPR.
[495] Recital 50 sentence 4 GDPR.
[496] Recital 65 sentence 5 GDPR.
[497] EDPS, "Preliminary Opinion on Data Protection and Scientific Research", 6 January 2020, p. 23.
[498] Ducato, "Data Protection, Scientific Research, and the Role of Information", Computer Law & Security Review 37 (2020) 105412, p. 5.

7.1.2.2.2. Derogations to Data Subject Rights

While derogations to the rights of the data subject can also be introduced by Union and by Member States law, the presentation here focuses predominantly on the derogations within the GDPR:

The derogation in Art. 14(5)(b) GDPR to the right to be provided information according to Art. 14(1) and 14(2) GDPR requires a balancing assessment. First, the impossibility and disproportionate effect of providing the required information has to be tailored to the number of data subjects, the age of the data and any appropriate safeguards.[499] Second, the controller has to evaluate the effort involved to provide the information to data subjects against the impact and effects on the data subject if they are not provided with the information.[500]

The derogation in Art. 17(3)(d) GDPR to the right to erasure[501] requires the data subject's exercise of this right to render impossible or seriously impair the achievement of the purposes privileged in Art. 89 GDPR. Resolving the conflict with the data subject's interests in favour of scientific research and statistics appears justified because any erasure of data used in scientific research or statistics would risk undermining the scientific validity of research by preventing verification of its results.[502]

The derogation in Art. 21(6) GDPR to the right to object[503] requires the processing for the purposes privileged in Art. 89 GDPR to be necessary for the performance of a task carried out for reasons of public interest. Consequently, the particular situation of an individual leading to an objection to processing can be limited by law for a superior interest of the public.

Art. 89(2) GDPR outlines the more specific conditions under which EU or Member State law may derogate from the data subject's right of access (Art. 15), right to rectification (Art. 16), right to restriction (Art. 18) and right to object (Art. 21). Such derogations are only possible if the conditions and safeguards required in Art. 89(1) GDPR are satisfied and are permitted insofar as they are necessary and proportionate in a democratic society to safeguard public security which also includes the prevention, investigation and prosecution of criminal offences.[504] In order to verify legitimate grounds for introducing such a derogation, Art. 89(2) GDPR establishes a 'three-step-test': (i) Exercising the respective right must be likely to render impossible or seriously impair the achievement of the purposes privileged in Art. 89(2) GDPR which include scientific research and statistics; (ii) the derogation has to be necessary for the fulfilment of these purposes; and (iii) appropriate safeguards have to be adopted for the data subject's rights and freedoms.

Considering that any restriction of data subject's rights needs to be in accordance with the requirements set out in the Charter of Fundamental Rights and in the ECHR,[505] it seems appropriate to point out that the right of access (Art. 15 GDPR) and the right to rectification (Art. 16 GDPR) are set out in Art. 8(2) Charter of Fundamental Rights itself. Because the right of access enables the data subjects to exercise the other rights provided for by data protection legislation, these two rights are generally considered essential components of

[499] Recital 60 sentence 2 and 3 GDPR.
[500] EDPS, "Preliminary Opinion on Data Protection and Scientific Research", 6 January 2020, p. 20, quoting Article 29 Working Party, Guidelines on transparency under regulation 2016/679, WP260, adopted on 29 November 2017 and last revised on 11 April 2018, pp. 28-31.
[501] Also known as the 'right to be forgotten'.
[502] Ducato, "Data Protection, Scientific Research, and the Role of Information", Computer Law & Security Review 37 (2020) 105412, p. 6.
[503] The right to object can be invoked only when the processing is based on the legitimate interest of the controller, Art. 21(1) GDPR.
[504] Recital 73 sentence 1 GDPR.
[505] Recital 73 sentence 2 GDPR.

the fundamental right to the protection of personal data and any derogation from these essential data subject rights must be subject to a particularly high level of scrutiny in line with the standards required by Art. 52(1) Charter of Fundamental Rights.[506]

7.1.2.2.3. Legal Bases for Processing for Privileged Purposes

Processing data for the purposes privileged in Art. 89 GDPR does not constitute *per se* a lawful basis for processing. Rather, the controller has to rely on one of the legal bases provided in Art. 6(1) GDPR and to ensure the fulfilment of the requirements set out in Art. 9 GDPR. Out of the six possible legal bases for processing of personal data, three seem to suggest themselves in the context of data processing for the purposes privileged in Art. 89 GDPR: (i) *consent*, Art. 6(1)(a) GDPR; (ii) *public interest*, Art. 6(1)(e) GDPR; and (iii) *legitimate interests*, Art. 6(1)(f) GDPR.

Consent according to Art. 6(1)(a) GDPR constitutes the most recurrent legal basis for human participants in research projects and also serves as a safeguard by giving individuals more control and choice and thereby upholding society's trust in science.[507] In the context of Big Data however, consent does not appear to be the most reliable legal basis for data processing for the purposes privileged in Art. 89 GDPR, because the data subjects have the right to withdraw their consent upon which the legal basis of consent ceases to exist, Art. 7(3) GDPR. Therefore, the other two legal bases may appear more suitable.

Where Member State law has recognised processing of personal data for the purposes privileged in Art. 89 GDPR as necessary for the performance of a task carried out in the public interest,[508] Art. 6(1)(e) GDPR provides a suitable legal basis for scientific research and statistics. In January 2020, the EDPS has offered to facilitate the debate with civil liberties groups, the research community and the major tech companies regarding the creation of a 'public interest' legal basis for dominant companies to disclose (personal) data to researchers in accordance with Art. 6(3) GDPR and has already indicated that such 'public legal' basis would have to be accompanied by a rigorous proportionality test as well as appropriate safeguards against misuse and unlawful access.[509]

The third possible legal basis for processing personal data for the purposes privileged in Art. 89 GDPR are the legitimate interests of the controller or a third party, Art. 6(1)(f) GDPR. In light of the balancing text required by legitimate interest as legal basis, Recital 113 GDPR appears to weigh decisively in favour of third parties' interest. According to the fourth sentence of this Recital, the legitimate interests of society for an increase of knowledge should be taken into consideration for the purposes privileged in Art. 89 GDPR. However, the legitimate interest legal basis requires a case-by-case evaluation and has to be as granular as possible, so that the controller is able to justify its decision in the light of the principle of accountability.[510]

Concerning the processing of special categories of data for the purposes privileged in Art. 89 GDPR, Art. 9 GDPR does not provide an alternative legal basis, but rather requires specific conditions in addition to Art. 6

[506] EDPS, "Preliminary Opinion on Data Protection and Scientific Research", 6 January 2020, p. 21.
[507] EDPS, "Preliminary Opinion on Data Protection and Scientific Research", 6 January 2020, p. 19.
[508] As an example for national law in accordance with Art. 6(3) GDPR see: Section 4(3) of the Finnish Data Protection Act (1050/2018), https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf.
[509] EDPS, "Preliminary Opinion on Data Protection and Scientific Research", 6 January 2020, p. 26.
[510] Ducato, "Data Protection, Scientific Research, and the Role of Information", Computer Law & Security Review 37 (2020) 105412, p. 7 and 8.

GDPR.[511]

Article 5 GDPR – Principles relating to processing of personal data

(1) Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6 GDPR – Lawfulness of processing

(1) Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller

[511] Recital 51 sentence 5 GDPR.

is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

(2) Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

(3) The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

(4) Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal

convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 9 GDPR – Processing of special categories of personal data

(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

(2) Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to

contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(3) Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

(4) Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 14 GDPR – Information to be provided where personal data have not been obtained from the data subject

(1) Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) *the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*

(b) *where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*

(c) *the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;*

(d) *where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*

(e) *the right to lodge a complaint with a supervisory authority;*

(f) *from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;*

(g) *the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*

(3) The controller shall provide the information referred to in paragraphs 1 and 2:

(a) *within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;*

(b) *if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or*

(c) *if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.*

(4) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

(5) Paragraphs 1 to 4 shall not apply where and insofar as:

(a) *the data subject already has the information;*

(b) *the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;*

(c) *obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data*

subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15 GDPR – Right of access by the data subject

(1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

(3) The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(4) The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Article 16 GDPR – Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means

of providing a supplementary statement.

Article 17 – Right to erasure ('right to be forgotten')

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18 – Right to restriction of processing

(1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) *the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;*

(b) *the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;*

(c) *the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;*

(d) *the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.*

(2) *Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.*

(3) *A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.*

Article 21 GDPR – Right to object

(1) *The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.*

(2) *Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.*

(3) *Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.*

(4) *At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.*

(5) *In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.*

(6) *Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.*

Article 89 GDPR – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

(1) Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

(2) Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

(3) Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

(4) Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

7.2. After-Roll-Out Phase: Use of GRACE Tools & Platform by LEAs

With the help of the analytical tools and the platform developed by the GRACE project, LEAs within the EU can gain much needed capacity to address the backlog in reports of CSEM referred to them. A semi-automated mechanism is envisioned to analyse and prioritise the content of the CSEM reports as well as to provide actionable intelligence for the protection of victims and for the apprehension of offenders. The Federated GRACE (Machine) Learning Platform is intended to create a unified learning infrastructure keeping pace with evolving trends in CSE as well as in the use of CSEM for the benefit of law enforcement across the EU without making the actual CSEM of a report available to LEAs with no jurisdiction. The workflow for CSEM reports is currently envisioned for the EU as follows:

- *External Reports:* CSEM reports from outside the EU enter the GRACE platform on a central server at Europol where they are enriched by the GRACE tools with several categorisations and made machine readable. Each enriched CSEM report is then forwarded only to the concerned national LEAs the jurisdiction of which have been identified as relevant by the GRACE system, while a copy of the enriched report is retained in a database.
- *Internal Reports:* A national LEA participating in the GRACE platform can also be an entry point for a

CSEM report. The workflow for national CSEM reports is similar to the workflow for reports from outside the EU, but it will not involve forwarding a copy of the national report to the central server at Europol. Rather, the national report is enriched locally by the same GRACE tools with the same categorisations and made machine readable after which the enriched national report is forwarded only to other national LEAs the jurisdiction of which has been identified by the GRACE system while only the extracted metadata of the national report is shared with the federated GRACE system.

The GRACE platform and tools (= the GRACE system) are envisioned only for analysing, categorising and managing the data contained in the CSEM reports. From a purely investigative point of view however, it would appear helpful for LEAs if the GRACE platform had also some tools integrated for searching the surface web as well as the dark web. Once a CSEM report is uploaded onto the GRACE system, such tools could automatically either (i) be restricted to verify the data contained in the CSEM report and to update as well as supplement the CSEM report or (ii) search independently of any existing CSEM report, continuously for new CSE(M) related content creating new reports of its own. Because of the investigative necessity to verify and the convenience to update the data contained in a CSEM report at some stage, it appears not unlikely that the GRACE platform may be combined with such search tools at some point in the future. The technological design of the GRACE platform cannot prevent a later combination with suitable search tools and, in that sense, will be open for being combined with such automatic search tools for investigative evidence. For that reason, it seems appropriate to include the data protection regime related to a combination with a search tool in the analysis presented in this section, even though the development and integration of such search tools in the GRACE platform is not part of the GRACE project.

Under both the CoE framework and the EU framework, LEAs will not be able to investigate crimes without specific laws in place authorizing such investigation.[512] In order to carry out the investigations LEAs need to be able to base their investigations on procedural instruments that enable them to take the measures that are necessary to identify an offender and collect the evidence required for the criminal proceedings.[513] These measures can be the same ones that are undertaken in other investigations not related to Internet-related content. However, investigating activities of criminals or criminal networks regarding CSEM online goes along with some unique challenges. As a consequence, investigations may be carried out in a different way compared to traditional investigations.[514] If an offender is for example based in one country[515], uses services

[512] This was highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

[513] Regarding user-based approaches in the fight against cybercrime, see: *Goerling*, The Myth Of User Education, 2006, at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[514] Due to the protocols used in Internet communication and worldwide accessibility, there is very little need for a physical presence at the place where a service is physically offered. Due to this independence of place of action and the crime site, many criminal offences related to the Internet are transnational crimes.

[515] The pure fact that the offender is acting from a different country can result in additional challenges for LEAs' investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases, the investigation nevertheless requires international cooperation

that enable anonymous communication and, in addition, propagates CSEM online by using different public Internet terminals, the identification of the suspect can hardly be based on traditional instruments like search and seizure alone.

7.2.1. CoE Framework

With regard to criminal investigations related to criminal use of the Internet for CSE purposes, the Council of Europe Convention on Cybercrime contains a set of provisions that reflect widely accepted minimum standards regarding procedural instruments required for online investigations.[516] The Convention on Cybercrime even addresses issues of high relevance – such as the question whether LEAs are allowed to access information available on servers located in another country. This seems especially relevant for criminal investigations concerning CSEM.

7.2.1.1. Fundamental Principles

The reference in Art. 15(1) CoE Convention on Cybercrime to the ECHR includes the protection of the right to respect for one's private and family life as well as one's home and correspondence enshrined in Art. 8 ECHR which appears most relevant for cybercrime investigations concerning CSEM. The concepts of "private life" and "correspondence" within the meaning of Art. 8(1) ECHR aim to protect the confidentiality of communications in a wide range of different situations covering mobile telephone communications[517] as well as other technologies, in particular electronic messages including emails[518] as well as Internet use[519], and data stored on computer servers[520]. All forms of interception, monitoring and seizure concerning these communications fall within the scope of Art. 8 ECHR.[521]

To ensure the protection of privacy granted in Art. 8 ECHR, the *European Court of Human Rights* (ECtHR) has developed a body of case law defining more precisely the standards that govern digital investigations. This body of case law seems today one of the most important sources for international standards in respect to

between the authorities in both countries, which in general is more time consuming compared to investigations concentrating on a single country.

[516] See Articles 15-21 of the Council of Europe Convention on Cybercrime.

[517] ECtHR, decision of 4 December 2015 in case of *Roman Zakharov v. Russia,* Application No. 47143/06, at para. 173; between family members, see ECtHR, decision of 20 January 1992 in case of *Margareta and Roger Andersson v. Sweden*, Application No. 12963/87, at para. 72; or with others, see ECtHR, decision of 15 June 1992 in case of *Lüdi v. Switzerland*, Application No. 12433/86, at para. 38 and 39.

[518] ECtHR, decision of 5 September 2017 in case of *Bărbulescu v. Romania* [GC], Application No. 61496/08, at para. 72; ECtHR, decision of 3 April 2007 in case of *Copland v. the United Kingdom*, Application No. 62617/00, at para. 41.

[519] ECtHR, decision of 3 April 2007 in case of *Copland v. the United Kingdom*, Application No. 62617/00, at para. 42.

[520] ECtHR, decision of 16 October 2007 in case of *Wieser and Bicos Beteiligungen GmbH v. Austria*, Application No. 74336/01, at para 45.

[521] ECtHR, "Guide on Article 8 of the European Convention on Human Rights", 20 August 2020, at para. 487.

investigations related to communication.[522] The body of case law takes particularly into consideration the *gravity* of interference of the investigation,[523] the *purpose* of the interference of the investigation,[524] and the *proportionality* of the interference of the investigation.[525] The following four fundamental principles can be extracted from the ECtHR's body of case law:

- The need for a *sufficient legal basis* for investigation instruments.[526]
- The requirement that the legal basis must be clear with regard to the *rights of a suspect*.[527]
- The *competences of LEAs* need to be foreseeable.[528]
- The surveillance of communication can only be justified in *context of serious crime*.[529]

In addition to these fundamental principles, Article 15(1) CoE Convention on Cybercrime expressly refers to the *principle of proportionality* which creates for Parties who are not Member States of the Council of Europe an obligation to develop the necessary safeguards.[530] Surveillance measures regarding communication may only be ordered if there is no prospect of successfully establishing the facts by another method or this would be considerably more difficult.[531]

[522] Gercke, "Understanding Cybercrime: phenomena, challenges and legal response", ITU 2012, at 6.5.3, p. 245.

[523] ECtHR, decision of 12 April 1990 in case of *Kruslin v. France*, Application No. 11801/85, at para. 33.

[524] ECtHR, decision of 26 April 1985 in case of *Malone v. United Kingdom*, Application No. 8691/79, at para. 67.

[525] ECtHR, decision of 6 September 1978 in case of *Klass and others v. Germany*, Application No. 5029/71, at para. 42.

[526] ECtHR, decision of 12 April 1990 in case of *Kruslin v. France*, Application No. 11801/85, at para. 27; ECtHR, decision of 24 April 1990 in case of *Huvig v. France*, Application No. 11105/84, at para. 32.

[527] ECtHR, decision of 4 December 2015 in case of *Roman Zakharov v. Russia,* Application No. 47143/06, at para. 229 et seq.; ECtHR, decision of 27 April 2004 in case of *Doerga v. The Netherlands*, Application No. 50210/99, at para. 50.

[528] ECtHR, decision of 15 April 2015 in case of *Dragojević v. Croatia*, Application No. 68955/11, at para. 94; ECtHR, decision of 12 April 1990 in case of *Kruslin v. France*, Application No. 11801/85, at para. 27 and ECtHR, decision of 26 April 1985 in case of *Malone v. United Kingdom*, Application No. 8691/79, at para. 67.

[529] ECtHR, decision of 15 April 2015 in case of *Dragojević v. Croatia*, Application No. 68955/11, at para. 94; ECtHR, decision of 6 September 1978 in case of *Klass and others v. Germany*, Application No. 5029/71, at para. 42.

[530] Gercke, "Understanding Cybercrime: phenomena, challenges and legal response", ITU 2012, at 6.5.3, p. 245.

[531] ECtHR, decision of 15 April 2015 in case of *Dragojević v. Croatia*, Application No. 68955/11, at para. 94.

7.2.1.2. Minimum Safeguards

Article 15(2) CoE Convention on Cybercrime supplements these five fundamental principles with an explicit reference to some of the most relevant safeguards including independent supervision, grounds justifying an application, and the limitation of the scope and the duration of such power or procedure.[532] One guarantee of an appropriate procedure designed to ensure that surveillance measures regarding communication are not ordered haphazardly, irregularly or without due and proper consideration in criminal investigations is to confine such measures to cases in which there are factual grounds for suspecting a person of planning, committing or having committed certain serious criminal acts.[533] Furthermore and in order to limit the power (and its potential abuse) which might be exercised by national authorities, the ECtHR has developed the following six minimum safeguards that must be set in national law: (1) the nature of offences which may give rise to an interception order; (2) the definition of the categories of people liable to have their communications intercepted; (3) the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) precautions to be taken when communicating the data to other parties and (6) circumstances in which recordings may or must be erased or destroyed.[534]

All in all, the system of safeguards required by the CoE Convention on Cybercrime combines the ability of LEAs to use the instruments provided in Art. 14 – 21 CoE Convention on Cybercrime in a flexible way with the guarantee of effective safeguards and depends on the implementation of a graded system of safeguards. The decision which safeguard needs to be implemented with regards to which instrument is left to the national legislators of the Parties.[535] The ability to ensure an adequate protection of the rights of a suspected individual within a graded system of safeguards largely depends on how the potential impact of an investigation instrument is balanced with the related safeguards at national level.

Title 1 – Common provisions

Article 14 CoE Convention on Cybercrime – Scope of procedural provisions

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

(2) Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;

(b) other criminal offences committed by means of a computer system; and

(c) the collection of evidence in electronic form of a criminal offence.

[532] This list of most relevant safeguards in Article 15(2) CoE Convention on Cybercrime is not exclusive, see No. 146 of the Explanatory Report to the CoE Convention on Cybercrime.

[533] ECtHR, decision of 15 April 2015 in case of *Dragojević v. Croatia*, Application No. 68955/11, at para. 94.

[534] ECtHR, decision of 4 December 2015 in case of *Roman Zakharov v. Russia,* Application No. 47143/06, at para. 231.

[535] See No. 147 of the Explanatory Report to the CoE Convention on Cybercrime.

(3)

(a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

(b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

(i) is being operated for the benefit of a closed group of users, and

(ii) does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 CoE Convention on Cybercrime – Conditions and safeguards

(1) Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

(2) Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

(3) To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 CoE Convention on Cybercrime – Expedited preservation of stored computer data

(1) Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious

preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

(2) Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 CoE Convention on Cybercrime – Expedited preservation and partial disclosure of traffic data

(1) Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

(a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

(b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

(2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 CoE Convention on Cybercrime – Production order

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

(a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

(b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

(2) *The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

(3) *For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*

(a) *the type of communication service used, the technical provisions taken thereto and the period of service;*

(b) *the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*

(c) *any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.*

Title 4 – Search and seizure of stored computer data

Article 19 CoE Convention on Cybercrime – Search and seizure of stored computer data

(1) *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:*

(a) *a computer system or part of it and computer data stored therein; and*

(b) *a computer-data storage medium in which computer data may be stored*

in its territory.

(2) *Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.*

(3) *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:*

(a) *seize or similarly secure a computer system or part of it or a computer-data storage medium;*

(b) *make and retain a copy of those computer data;*

(c) *maintain the integrity of the relevant stored computer data;*

(d) *render inaccessible or remove those computer data in the accessed computer system.*

(4) *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the*

undertaking of the measures referred to in paragraphs 1 and 2.

(5) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 CoE Convention on Cybercrime – Real-time collection of traffic data

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

(a) collect or record through the application of technical means on the territory of that Party, and

(b) compel a service provider, within its existing technical capability:

(i) to collect or record through the application of technical means on the territory of that Party; or

(ii) to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 CoE Convention on Cybercrime – Interception of content data

(1) Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

(a) collect or record through the application of technical means on the territory of that Party, and

(b) compel a service provider, within its existing technical capability:

(i) to collect or record through the application of technical means on the territory of that Party, or

(ii) to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Update Legal Report v2:

7.2.1.3. Second Additional Protocol to Budapest Convention

While the Coe Convention on Cybercrime provides for the cross-border collection and exchange of information and evidence for specific criminal investigations or proceedings,[536] the Second Additional Protocol[537] is intended to bring the CoE Convention on Cybercrime in line with other international instruments including the 2013 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[538], GDPR and Law Enforcement Directive in the EU, and the African Union Convention on Cyber Security and Personal Data Protection[539] ("Malabo Convention"). Because the Second Additional Protocol is open for signature to State Parties which are neither subject to CoE data protection instruments nor EU data protection rules, the Second Additional Protocol aims to provide a balance reflective of the many legal systems of countries likely to become State Parties while respecting the importance of ensuring the protection of privacy and personal data as required by the constitutions and international obligations of existing State Parties.[540]

The Second Additional Protocol of the CoE was opened for signature in May 2022. Since then, 37 countries, latest Mauritius, have signed it. Five of these states have also ratified the protocol. For the entry into force it

[536] Section 2.2 above presents the legal framework for cross-border cooperation under the CoE Convention on Cybercrime.
[537] CoE, Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Draft Protocol version 2, 12 April 2021. Section 2.2.5 above presents the methods of international co-operation envisioned under the Second Additional Protocol.
[538] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980, available at: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.
[539] African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014, available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.
[540] CoE, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Special Edition of 17 November 2021, Explanatory Report, para. 23 and 44, p. 37 et seq., available at: https://rm.coe.int/special-edition-second-protocol-en-2021/1680a69930.

is required that the Second Additional Protocol of the CoE has been ratified by 5 states. The European Parliament decided on January 17, 2023, that member states of the EU may ratify the convention.[541]

Whenever personal data are transferred pursuant to the Second Additional Protocol, the comprehensive data protection safeguards of Art. 14 Second Additional Protocol will apply which regulate: (1) the scope; (2) the sole purpose and use of the data; (3) the quality and integrity of the data; (4) appropriate safeguards for sensitive data; (5) retention periods; (6) the prohibition of automated decisions; (7) requirements of data security and handling of security incidents; (8) records demonstrating how personal data of an individual is processed; (9) how data may be shared within a State Party; (10) how data may be transferred to another State Party; (11) transparency and notice to the data subject; (12) access and rectification rights for the data subject; (13) judicial and non-judicial remedies providing redress for data protection violations; (14) oversight mechanisms ensuring data protection compliance; and (15) consultation and suspension mechanisms concerning State Parties found in breach of data protection requirements.

7.2.2. EU Framework

Within the EU, data protection in the police and criminal justice sector is regulated in the context of both national and cross-border processing by police and criminal justice authorities of the Member States and EU actors. The central instrument at EU level is Directive (EU) 2016/680[542] which aims to protect personal data collected and processed for criminal justice purposes including prevention, investigation, detection or prosecution of criminal offences.

7.2.2.1. Applicability to Criminal Investigation

Art. 51 Charter of Fundamental Rights demands the Member States of the EU to respect the rights and to observe the principles laid down in the Charter of Fundamental Rights only when they are implementing Union law. Member States are implementing Union law when national legislation falls within the scope of European Union law which automatically opens the jurisdiction of the *Court of Justice of the European Union* (CJEU) to guide the interpretation of the Charter of Fundamental Rights so that national courts can determine whether a national legislation is compatible with the fundamental rights enshrined in the Charter of Fundamental Rights.[543]

In case LEAs use the GRACE tools and platform in criminal investigations including for searching the Internet and the dark web for evidence, the protection of privacy and personal data is crucial for individuals whose activities and connections are examined.

[541] See: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0002_EN.html.
[542] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the EU, L 119/89, 4 May 2016.
[543] CJEU, decision of 26 February 2013 in case *Akerberg Fransson*, C-617/10, at para. 19.

- **Exemptions in GDPR and ePrivacy Directive**

Most relevant for the guarantees of the right to respect for private and family life[544] and the right to protection of personal data[545] is Art. 2(2)(d) GDPR[546] which provides an exemption for LEAs investigating criminal offences from the scope of the GDPR and causes such investigations to fall under Union law.

The ePrivacy Directive ensures the protection of the fundamental right to respect for private and family life, the confidentiality of communications and the protection of personal data in the electronic communications sector. It also guarantees the free movement of electronic communications data, equipment and services in the Union. It implements in the Union's secondary law the fundamental right to the respect for private life, with regard to communications, as enshrined in Art. 7 Charter of Fundamental Rights. According to its Art. 1(3), the ePrivacy Directive shall not apply in any case to activities concerning (among others) public security and the activities of the State in areas of criminal law. This exemption for LEAs from the scope of the ePrivacy Directive also causes monitoring of online activities to fall under Union law.

Because consumers and businesses increasingly rely on internet-based services enabling inter-personal communications such as Voice over IP, instant messaging and web-based e-mail services, instead of traditional communications services, the European Commission proposed an ePrivacy Regulation[547] on 10 January 2017. However, the proposed ePrivacy Regulation is not envisaged to apply to activities of LEAs "for the purposes of the prevention, investigation, detection or prosecution of criminal offences" according to Art. 2(2)(d) ePrivacy Regulation. While the European Parliament left this exemption unaltered in its report of 20 October 2017,[548] the Council of the EU explicitly added "including data processing activities" to this exemption in its mandate for negotiations with the European Parliament adopted on 10 February 2021.[549] The legislative process is currently at the trilogue stage and it seems most probably that the exemption for LEAs monitoring online activities in the course of a criminal investigation will remain. Therefore, this exemption of activities of LEAs from the scope of the proposed ePrivacy Regulation will perpetuate that monitoring of online activities falls under Union law.

In this context, it is interesting to note that Over-the-Top communications services ("OTTs") had in general

[544] Art. 7 Charter of Fundamental Rights.

[545] Art. 8 Charter of Fundamental Rights.

[546] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal L 119/1, 4 May 2016.

[547] European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 10 January 2017.

[548] European Parliament, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), A8-0324/2017, 20 October 2017.

[549] Council of the EU, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003(COD), 6087/21, 10 February 2021.

been subject only to the GDPR and not to the Union electronic communications framework, including the ePrivacy Directive. This has changed in December 2020 when the comprehensive European Electronic Communications Code (EECC)[550] entered into application, bringing with it a new definition of electronic communications services in Art. 2(4) EECC. This definition encompasses 'number-independent interpersonal communications services' (NI-ICS),[551] which includes messaging services. As the ePrivacy Directive relies on the definition of electronic communications services in the EECC, NI-ICS are subject to the confidentiality rules of the ePrivacy Directive. In contrast to the GDPR, the ePrivacy Directive does not contain a legal basis for the voluntary processing of content or traffic data for the purpose of detecting child sexual abuse. Therefore, for services falling within the scope of the ePrivacy Directive, a specific derogation to Art. 5(1) and 6(1) ePrivacy Directive has been agreed upon by the negotiators from the Council and the European Parliament as temporary measure to allow providers of electronic communications services such as web-based email and messaging services to continue to detect, remove and report child sexual abuse online, also covering anti-grooming, until permanent legislation announced by the European Commission is in place.[552] The negotiated interim Regulation[553] will apply for three years, or until an earlier date if the permanent legal instrument is adopted by the legislators and repeals these temporary rules before then.

- **Restrictions on Freedom Provided in TFEU**

The applicability of the Charter of Fundamental Rights also results from the fact that acts of online monitoring may affect the prohibition of restrictions on the freedom to provide services within the EU in Art. 56 of Treaty of Functioning of the European Union (TFEU).[554] According to the CJEU, even in a situation where action of a Member States is only partially determined by EU law, the "implementation" requirement of Art. 51(1) Charter of Fundamental Rights is met whenever a national court is called upon to review whether fundamental rights are complied with by a national provision or measure.[555]

[550] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, Official Journal of the EU, L 321/36, 17.12.2018 which is applicable since 21 December 2020.
[551] Art. 2(7) EECC.
[552] Council of the EU, "Combating child abuse online – informal deal with European Parliament on temporary rules", 29 April 2021, available at: https://www.consilium.europa.eu/en/press/press-releases/2021/04/29/combating-child-abuse-online-informal-deal-with-european-parliament-on-temporary-rules.
[553] Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, COM(2020) 568 final, 10 September 2020.
[554] CJEU, decision of 26 February 2013 in case *Akerberg Fransson*, C-617/10, at para. 29.
[555] CJEU, decision of 26 February 2013 in case *Akerberg Fransson*, C-617/10, at para. 29.

7.2.2.2. Lines of Case Law Synchronising Privacy Protection under Charter of Fundamental Rights and under ECHR

In the area of privacy and data protection, the CJEU has developed a line of case law which expounds Art. 7 and 8 Charter of Fundamental Rights in combination with Art. 8 ECHR and refers to the established line of case law by the ECtHR on the guarantee of privacy under the ECHR.[556] In this context, it has to be pointed out that also the ECtHR refers in its more recent case law to the principles developed by the CJEU regarding the interpretation of Art. 7 and 8 Charter of Fundamental Rights.[557] This kind of cross-referencing to each other's line of case law appears to be a rather recent phenomenon but allows, nevertheless, to expect a uniform interpretation of the protection of privacy in the future.[558]

- **Minimum Standards for Privacy Protection**

Furthermore, the CJEU expressly mentions "minimum safeguards" for individuals against the risk of abuse and unlawful access of data retained by LEAs in their fight CSE.[559] With these "minimum safeguards", the CJEU refers to the line of case law of the ECtHR described at section 5.2.1.2. above establishing coherent minimum standards for national surveillance measures without formulating its own detailed catalogue of minimum requirements. This reference to the ECtHR's line of case law leads to the conclusion that the cumulative minimum standards established by the ECtHR are to be applied under the Charter of Fundamental Rights as well. Indeed, the CJEU goes on to examine each of the exact criteria developed by the ECtHR:

- Restrictions of individuals affected by the surveillance measure;[560]
- Access restrictions to collected data to ensure their availability for serious crimes only;[561]
- Limitation of data retention period;[562] and
- Guarantee of data security.[563]

According to the CJEU, the retention of surveillance data requires an explicit reason for the collection of the

[556] CJEU, decision of 21 December 2016 in case *Tele2 Sverige AB,* C-203/15 and C-698/15, at paras. 119 and 120; CJEU, decision of 8 April 2014 in case *Digital Rights Ireland*, C-293/12 and C-592/12, at para. 35, 47, 54.

[557] ECtHR, decision of 12 January 2016 in case of *Szabo and Vissy v. Hungary*, Application No. 37138/14, at para. 68, 70, 73: ECtHR, decision of 4 December 2015 in case of *Zakharov v. Russia*, Application No. 47143/06, at para. 147.

[558] Boehm/Andrees, CR 2016, pp. 146-154.

[559] CJEU, decision of 8 April 2014 in case *Digital Rights Ireland*, C-293/12 and C-592/12, at para. 54.

[560] CJEU, decision of 8 April 2014 in case *Digital Rights Ireland*, C-293/12 and C-592/12, at para. 58.

[561] CJEU, decision of 8 April 2014 in case *Digital Rights Ireland*, C-293/12 and C-592/12, at para. 60.

[562] CJEU, decision of 8 April 2014 in case *Digital Rights Ireland*, C-293/12 and C-592/12, at para. 63.

[563] CJEU, decision of 8 April 2014 in case *Digital Rights Ireland*, C-293/12 and C-592/12, at para. 66.

data[564] and creates a need for a threat to public security causing the collection of data.[565]

As a result, the protection of the right to respect for private and family life[566] and of the right to protection of personal data[567] under the Charter of Fundamental Rights appears currently fully synchronised with the protection of the right to respect for private and family life[568] under the ECHR.

7.2.2.3. Directive (EU) 2016/680 for Data Protection in the Police and Criminal Justice Sectors

On 5 May 2016, Directive (EU) 2016/680 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data[569] entered into force and Member States had to transpose it into their national law by 6 May 2018. Directive (EU) 2016/680 is applicable to national LEAs in Member States.

- **Legislative Competence of the European Union**

Directive (EU) 2016/680 was adopted in order to ensure a high level of data protection while improving cooperation in the fight against CSE and other serious crime. After the Treaty of Lisbon came into effect, the protection of natural persons in relation to the processing of personal data is expressly recognized as a fundamental right. Article 8(1) Charter of Fundamental Rights and Article 16(1) TFEU provide that everyone has the right to the protection of personal data concerning him or her. However, Declaration 21, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, acknowledges that the specific nature of the security field merits special legislative treatment. According to the European institutions' approach, processing in the police and criminal justice context should be differentiated from all other personal data processing. The protection and free movement of data processed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties has been regulated by a directive, allowing Member States a certain level of flexibility while incorporating it into their respective national laws.

- **Brief Overview of Contents**

Directive (EU) 2016/680 aims at balancing the data protection objectives with the security policy objectives

[564] CJEU, decision of 8 April 2014 in case *Digital Rights Ireland*, C-293/12 and C-592/12, at para. 58.

[565] CJEU, decision of 8 April 2014 in case *Digital Rights Ireland*, C-293/12 and C-592/12, at para. 59.

[566] Art. 7 Charter of Fundamental Rights.

[567] Art. 8 Charter of Fundamental Rights.

[568] Art. 8 ECHR.

[569] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the EU, L 119/89, 4 May 2016.

and, while certainly contributing to the creation of a less fragmented general framework, it does not solve all the shortcomings which had emerged before its adoption. Directive (EU) 2016/680 comprises ten chapters which can be divided into two parts:

The **first part** of Directive (EU) 2016/680 consists of chapters I – V which describe:

- the scope,[570]
- the general principles relating to processing of personal data,[571]
- the rights of the data subject,[572]
- the obligations of the controllers and the processors,[573] the technical and organizational measures to ensure security of personal data, which have to be adopted by them,[574] as well as the designation of a data protection officer,[575] and
- the regulation of transfer of personal data to third countries or international organizations.[576]

The **second part** of Directive (EU) 2016/680 regulates:

- the independent status,[577] the competence, tasks and powers[578] of the independent supervisory authorities and establishes the right to lodge a complaint with a supervisory authority,
- the cooperation between Member States by mutual assistance,[579]
- the right to an effective judicial remedy against a controller or processor and the right to compensation for any person who has suffered material or non-material damage as a result of an unlawful processing of personal data.[580]

- **Scope**

Directive (EU) 2016/680 applies to the processing of personal data by competent authorities "for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties", Article 2(1) Directive (EU) 2016/680 in connection with Art. 1(1) Directive (EU) 2016/680. The use

[570] Art. 1 – 3 Directive (EU) 2016/680, chapter I.

[571] Art. 4 – 11 Directive (EU) 2016/680, chapter II.

[572] Art. 12 – 18 Directive (EU) 2016/680, chapter III.

[573] Art. 19 – 28 Directive (EU) 2016/680, chapter IV, section 1.

[574] Art. 29 – 31 Directive (EU) 2016/680, chapter IV, section 2.

[575] Art. 32 – 34 Directive (EU) 2016/680, chapter IV, section 3.

[576] Art. 35 – 40 Directive (EU) 2016/680, chapter V.

[577] Art. 41 – 44 Directive (EU) 2016/680, chapter VI, section 1.

[578] Art. 45 – 49 Directive (EU) 2016/680, chapter VI, section 2.

[579] Art. 50 – 51 Directive (EU) 2016/680, chapter VII.

[580] Art. 52 – 57 Directive (EU) 2016/680, chapter VIII. The final two of Directive (EU) 2016/680 are about implementing acts, chapter IX, and final provisions, chapter X.

of the GRACE tools and platform in criminal investigations falls clearly within the scope of Directive (EU) 2016/680.

- **Data Processing in the Course of Criminal Investigations**

Directive (EU) 2016/680 protects the personal data of different categories of individuals involved in criminal proceedings, such as witnesses, informants, victims, suspects and accomplices. Police and criminal justice authorities are obliged to comply with the Directive's provisions whenever they process such personal data for law enforcement purposes, within both the personal and the material scope of Directive (EU) 2016/680. However, the use of data for a different purpose is also allowed under certain conditions. The processing of data for a different law enforcement purpose than that for which it was collected is only permitted if this is lawful, necessary and proportionate according to national or EU law.[581] For other purposes, the rules of the GDPR apply. The logging and documenting of data sharing is one of the competent authorities' specific duties to assist with the clarification of responsibilities arising from complaints.

It is interesting to note that Recital 49 Directive (EU) 2016/680 seems to suggest that where personal data are processed in the course of "a criminal investigation", Member States may provide for the exercise of the right to information[582], access[583] and rectification or erasure[584] of personal data to be carried out in accordance with their national law. Read together with Art. 18 as well as Recitals 20 and 107 Directive (EU) 2016/680, this appears to provide an opening for different national laws under the framework of Directive (EU) 2016/680. Because of this ambiguity, the real added value of Directive (EU) 2016/680 will depend on its implementation in national law and the willingness of national courts to ensure that Directive (EU) 2016/680 is applied in a uniform manner across the EU.

- **Data Processing Outside the Scope of Union Law**

Directive (EU) 2016/680 does not regulate the processing of data in the course of an activity which falls outside the scope of Union law, Art. 2(3)(a) Directive (EU) 2016/680. Recital 14 Directive (EU) 2016/680 suggests to interpret Article 2(3)(a) Directive (EU) 2016/680 as relating to activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU. As consequence, the wording of Article 2(3) Directive (EU) 2016/680 appears to be in conflict with the inclusion of "safeguarding against and the prevention of threats to public security" in Article 1(1) Directive (EU) 2016/680. The concept of activities concerning national security is not defined in Directive (EU) 2016/680, but seems to include "activities of safeguarding against and prevention of threats to public security". Until the CJEU will guide the interpretation of this contradiction, the scope of Directive (EU) 2016/680 will depend on the interpretation that national courts will give to the expression "activity which falls outside the scope of Union law" and of the way the Member States decide to implement Directive (EU) 2016/680.

- **Data Processing by EU Institutions, Bodies, Offices and Agencies**

[581] Art. 4(2) Directive (EU) 2016/680.
[582] Art. 13 Directive (EU) 2016/680.
[583] Art. 14 Directive (EU) 2016/680.
[584] Art. 16 Directive (EU) 2016/680.

Finally, Directive (EU) 2016/680 does not apply to the processing of personal data by the Union institutions, bodies, offices and agencies, Art. 2(3)(b) Directive (EU) 2016/680. The data processing by the European institutions and bodies is governed by Regulation (EU) 2018/1725 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement.[585] Regulation (EU) 2018/1725 aims to bring the level of data protection at EU institutions, bodies, offices and agencies in line not only with the GDPR but also with Directive (EU) 2016/680.[586]

Europol was established in 1998 and its present legal status as an EU institution is based on the Regulation on the European Union Agency for Law Enforcement Cooperation (Europol Regulation).[587]

- **Minimum Harmonisation within the EU**

Directive (EU) 2016/680 regulates the processing of personal data by Member States and not only intra-Member States exchanges of data. Nevertheless, Directive (EU) 2016/680 is still far from ensuring maximum harmonisation of data processing in the criminal field. Art. 1(3) Directive (EU) 2016/680 states that Directive (EU) 2016/680 shall not preclude Member States from providing higher safeguards than those established in Directive (EU) 2016/680 for the protection of the rights and freedoms of the data subject. As a result, Directive (EU) 2016/680 ensures only a minimum harmonisation.

- **Comparison of Principles for Data Processing with GDPR**

Several principles relating to processing of personal data are the same as those enshrined in the GDPR. However, because of the peculiarity of the field, while the basic data protection principles are included in its text, some of those set out in the GDPR are not included in Directive (EU) 2016/680. For example:

As far as the *characteristics the data* should have in order to be processed by the competent authorities are concerned, it may be observed that not all the conditions required by the GDPR in order to consider the data processing lawful and fair need to be met under Directive (EU) 2016/680.

The *consent of the data subject* is not a necessary condition for processing personal data by the competent authorities according to Recital 35 Directive (EU) 2016/680 when they order natural persons to comply with requests made in order to perform the tasks of preventing, investigating, detecting or prosecuting criminal offences. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. Whether the correct balance between individual data protection and the interests of the

[585] European Commission, Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, 23 October 2018.

[586] Recitals 9 and 10 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM(2017) 8 final, 10 January 2017.

[587] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135, p. 53.

police and criminal justice process is respected depends once again on how Member States have implemented the exemptions contained in Directive (EU) 2016/680.

Directive (EU) 2016/680 also allows Member States to adopt legislative measures restricting the data subject's rights to information[588], access[589] and rectification[590] in an attempt to strike a balance between the individual right to data protection and the processing interests and concerns of the police and other LEAs. If exercised to their fullest extent these rights would undermine much of the work done by the police and the competent authorities within the criminal justice system. The level of flexibility accorded to this end depends once more on the breadth of national legislative measures implementing Directive (EU) 2016/680, which can restrict, wholly or partly, the data subject's right in order to assure the due performance of investigations and protect national security, as set out in Art. 15 Directive (EU) 2016/680.

- **Independent Supervisory Authority**

The final important element of the EU data protection model refers to the establishment of an independent supervisory authority entrusted with the task of monitoring the application of data protection law within the respective Member State. Directive (EU) 2016/680 permits assignment of this role to the authority established for similar purposes under the GDPR. Data Protection Authorities, as independent supervisory authorities, had been introduced by Data Protection Directive 95/46/EC and have become the basic mechanism for enforcement and monitoring of data protection in the EU.

The European Data Protection Board has replaced the former Article 29 Working Party and is assigned a central role by the GDPR (especially in the consistency mechanism), but no such role is provided for in Directive (EU) 2016/680. However, in the police and criminal justice context conflicts pertaining to processing of personal data may arise between the Data Protection Authority and the judicial authorities in order to determine whether a Data Protection Authority may monitor processing done by judicial authorities. In order to limit the discretionary power of the Member States, Directive (EU) 2016/680 provides that the processing of data by judicial authorities must not be affected by its provisions when acting within their judicial capacity. In spite of that Art. 1(3) Directive (EU) 2016/680 permits Member States to maintain a higher level of data protection which may ultimately be a cause of problems.

- **International Data Transfers**

Directive (EU) 2016/680 provides rules for international data transfers in its chapter V.

- **Data Transfers Among Member States**

Where personal data are to be transmitted or made available from another Member State, Art. 35 (1) Directive (EU) 2016/680 requires five enumerated conditions to be met including that the other Member State has to give its prior authorisation to the transfer in accordance with its national law[591]. However, according to Art. 35(2) Directive (EU) 2016/680 Member States shall provide for data transfers without prior authorisation by

[588] Art. 13(3) Directive (EU) 2016/680.

[589] Art. 15(1) Directive (EU) 2016/680.

[590] Art. 16(4) Directive (EU) 2016/680.

[591] Art. 35(1)(c) Directive (EU) 2016/680.

the other Member State to be permitted if, and only if, the data transfer is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country and the prior authorization cannot be obtained in good time. In these scenarios, the second sentence of Art. 35 (2) Directive (EU) 2016/680 requires that the authority which is responsible for giving prior authorization has to be informed without delay.

- **Data Transfers to Third Countries**

With regard to the transfer of personal data to third countries or international organisations Art. 36 (1) Directive (EU) 2016/680 requires that personal information be allowed to be transmitted by a Member State to a third country only if the Commission has decided that the recipient ensures an "adequate" level of protection. The concept of adequate level of protection has been defined by the CJEU in the cases of *Schrems I*[592] and *Schrems II*[593] as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU. The CJEU has also stated that the European Commission's discretion as to the adequacy of the level of protection ensured by a third Country should be limited, considering, *first*, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, *secondly*, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country without ensuring an adequate level of protection.[594]

In that respect it should be underlined that data processing in the police and criminal justice context was up until 2018 a field left outside Union law. Practically all Member States have bilateral agreements with third countries permitting the exchange of personal data for law enforcement related purposes, notwithstanding any "adequacy" finding in respect of the recipients' data protection safeguards. Therefore, here again Directive (EU) 2016/680 had to maintain a careful balance between, on the one hand, the requirements of police and criminal justice work and existing bilateral agreements and, on the other, the requirement for an increased level of personal data protection.

Directive (EU) 2016/680 appears to do little to affect bilateral agreements which are already in place. As a consequence, Directive (EU) 2016/680 automatically turned all bilateral agreements into definite term ones needing amendment to match its standards. However, if Member States – that are called upon, but not obliged to actively seek to amend bilateral agreements in the foreseeable future[595] – have not taken action, the prolonged existence of those bilateral agreements which apply lower standards than Directive (EU) 2016/680 seems to undermine the whole international data transfer edifice.

- **Profiling**

The regulation of profiling in Directive (EU) 2016/680 deserves a separate mention. Profiling is especially problematic in the police and criminal justice context because if profiles are misused they can lead to stressful situations for individuals who could be put under surveillance or arrested on the grounds of automated

[592] CJEU, decision of 6 October 2015 in case *Schrems*, C-362/14, CRi 2016, p. 25 at para. 73.

[593] CJEU, decision of 16 July 2020 in case *Schrems II*, C-311/18, Cri 2020, p. 109 at para. 105.

[594] CJEU, decision of 6 October 2015 in case *Schrems*, C-362/14, CRi 2016, p. 26 at para. 78; CJEU, decision of 8 April 2014 in case *Digital Rights Ireland*, C-293/12 and C-592/12, at para. 47 and 48.

[595] See Art. 40 Directive (EU) 2016/680.

processing of personal data. The compatibility with the presumption of innocence[596] may be questioned.

In this context, it is necessary to underline that Directive (EU) 2016/680 provides substantial and procedural safeguards. According to Art. 11(1) Directive (EU) 2016/680, Member States are prohibited from providing for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject. Art. 11(3) Directive (EU) 2016/680 also stresses that profiling resulting in discrimination against natural persons shall be prohibited.

Update for Legal Report v2:

7.2.2.4. Europol Regulation

The European Union Agency for Law Enforcement Cooperation (Europol) was established by Regulation (EU) 2016/794[597] (Europol Regulation). Six years later, the Europol Regulation was amended and Europol's mandate extended by Regulation (EU) 2022/991[598] (Amending Europol Regulation) in three respects: (1) Europol's cooperation with private parties, (2) Europol's processing of personal data in support of criminal investigations, and (3) Europol's role in research and innovation. The amended Europol Regulation (new) provides Europol with an expanded mandate with regard to exchanges of personal data with private parties,[599] the use of artificial intelligence,[600] and the processing of large datasets.[601]

This section provides an overview of the resulting amended Europol Regulation[602] and provides an insight as to why changes regarding the processing of personal data by Europol had become necessary. The reasons for the changes of the data protection regime governing Europol's processing of personal data inform the interpretation of the new provisions governing added by the Amending Europol Regulation.

---

[596] Art. 48 Charter of Fundamental Rights.

[597] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135, 24 May 2016, p. 53.

[598] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, OJ L 169, 27 June 2022, p. 1.

[599] Art. 18(2)(d) Europol Regulation (new).

[600] Europol's task to proactively monitor research and innovation activities includes includes projects „for the development, training, testing and validation of algorithms for the development of specific tools" for the use by LEAs, Art. 4(1)(v) Europol Regulation (new).

[601] Pursuant to Art. 51(3)(d) Europol Regulation (new), Europol's mandatory annual report to the Joint Parliamentary Scrutiny Group (JPSG) has to include relevant information on Europol's activities and results obtained in processing large data sets.

[602] Regarding Articles which have been changed by the Amending Europol Regulation, the previous version is indicated by „Europol Regulation (old)", whereas the current version as well as newly created Articles are indicated by "Europol Regulation (new). Articles of the Europol Regulation without the indication as "(old)" or "(new)" have remained unchanged by the Amending Europol Regulation.

- **Objectives**

The Europol Regulation (introduced in 2016) aims to achieve two objectives: The first objective is to facilitate information sharing from Member States to Europol, for instance through the automation of data transfers.[603] The second objective is to establish a data processing environment that will support Europol analysts in performing their tasks.[604] Consequently, the Europol Regulation ceased to implement purpose limitation by separating personal data into closed silos.[605] Rather, the Europol Regulation sought to enforce purpose limitation by attaching the safeguards directly to the data (e.g. using metadata).[606] The intention was to allow Europol processing of data in innovative ways, not limited by the underlying IT infrastructure, and acting as a service provider, in particular by providing a secure network for the exchange of data, via the secure information exchange network application (SIENA).[607]

As key restrictions to the use of the data, the Europol Regulation introduced an information structure focusing on the purposes for which data is being processed. Art. 18(2) Europol Regulation enables Europol to process personal data only for the following purposes: (a) cross-checking aimed at identifying connections between information related to crimes within Europol's mandate; (b) strategic or thematic analyses; (c) operational analyses; (d) facilitating exchanges of information between Member States, Europol and other EU bodies, as well as third countries and international organisations. This data processing approach offers a high degree of flexibility and increased information-related powers to Europol potentially enhancing Europol's operational effectiveness.

- **Operational Effectiveness and Data Protection Principles**

To achieve operational effectiveness, Europol needs to be able to legitimately use big data analytics. Although not explicitly mentioned, enabling Europol to cross-link data more easily, to identify patterns and risky behaviours had been identified as one of the Europol Regulation's main goals.[608]

The emphasis on operational effectiveness appears amplified by the requirement that Europol uses new technologies for data processing and most efficient IT infrastructures for its databases to swiftly detect links between investigations and common *modi operandi* across different criminal groups, to check cross-matches of data and to have a clear overview of trends.[609]

The policy objective of operational effectiveness appears antagonistic to the principles of purpose limitation and data minimisation. Both are core principles for data processing and require effective safeguards and controls. Furthermore, the possibility for Europol to cross-match data collected for different purposes and across different databases and the extended access to Europol data provided to Member States[610] seem

[603] Rec. (3), (12)-(15), (24) Europol Regulation.
[604] European Commission, Impact Assessment regarding Europol Regulation, SWD/2013/098 final, 27 March 2013.
[605] Previously, the focus was on the regulation of Europol's databases Europol Information Systems and Analysis Work Files.
[606] See Chapter VI Europol Regulation (old) on Data Protection Safeguards.
[607] Rec. (24) sentences 3 and 4 Europol Regulation.
[608] Coudert, "The Europol Regulation and purpose limitation: from the "silo-based approach" to …what exactly? (Part II)", 20 April 2017, available at: https://www.law.kuleuven.be/citip/blog/the-europol-regulation-and-purpose-limitation-from-the-silo-based-approach-to-what-exactly-part-ii/.
[609] Rec. (24) sentence 2 Europol Regulation.
[610] Art. 20 Europol Regulation (old).

problematic in the light of the data processing principles of necessity and proportionality.[611] As a result, the balance between core data protection principles and Europol's need for operational effectiveness creates a challenge.

- **Old Data Protection Safeguards and "Big Data Challenge"**

The data protection regime of the Europol Regulation (old) had established various safeguards: Art. 28(1) Europol Regulation (old) enshrined the five general principles of data protection:[612] (a) the principle of *'lawfulness, fairness and transparency'*; (b) the principle of *'purpose limitation'*;[613] (c) the principle of *'data minimisation'*; (d) the principle of *'accuracy'*;[614] (e) the principle of *'storage limitation'*; and (f) the principle of *'integrity and confidentiality'*[615]. Further safeguards included the assessment of reliability of the source of information[616] and the accuracy of information[617] as well as stricter rules for the processing of special categories of personal data,[618] time-limits for the storage and erasure of personal data,[619] technical and organisational measures for the security of processing[620] and for data protection by design.[621]

However, the safeguards laid down in Chapter VI. Europol Regulation (old) seemed to address the specific challenges brought by big data analytics somewhat insufficiently. The concept of purpose limitation relies on the premise that it is possible to decide on the purpose of specific data processing before the processing occurs, while the added value of big data technologies resides in their potential to uncover new correlations and knowledge.[622] In practice, the use of big data technologies does not require Europol to formulate a distinct hypothesis before querying the IT-system in the course of an investigation. Rather, the hypothesis is generated automatically by the big data technologies. Seen from this angle, purpose seems a most unlikely criterion for acting as a limit to the logic of data maximisation (the more data, the better the algorithm will perform) especially when big data analytics allow not only the processing of structured but also unstructured data.[623]

---

[611] Coman-Kund, "Europol's International Exchanges of Data and Interoperability of AFSJ Databases", European Public Law 26, no. 1 (2020), page 181 (at page 193).
[612] These general data protection principles incorporated the principles relating to processing of personal data enshrined in Art. 5 GDPR.
[613] Note that further processing of personal data for historical, statistical or scientific research purposes was not considered incompatible provided that Europol provided appropriate safeguards, in particular to ensure that data were not processed for any other purposes.
[614] Note that every reasonable step had to be taken to ensure that inaccurate personal data (having regard to the purposes for which they were processed) were erased or rectified without delay.
[615] Note that, in contrast to Art. 5 GDPR, the "protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures" was not expressively included in Art. 28(1)(f) Europol Regulation (old).
[616] Art. 29(1) Europol Regulation (old).
[617] Art. 29(2) Europol Regulation (old).
[618] Art. 30(1) and (2) Europol Regulation (old).
[619] Art. 31 Europol Regulation (old).
[620] Art. 32(1) and (2) Europol Regulation (old).
[621] Art. 33 Europol Regulation (old).
[622] Moerel/Prins, "Privacy for the homo digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things", 25 May 2016, page 7.
[623] Coudert, "The Europol Regulation and purpose limitation: from the "silo-based approach" to …what exactly? (Part II)", 20 April 2017, available at: https://www.law.kuleuven.be/citip/blog/the-europol-regulation-and-purpose-limitation-from-the-silo-based-approach-to-what-exactly-part-ii/.

Against this background, it does not appear surprising that Europol was faced by a "big data challenge". The term "big data challenge" refers to a decision by the European Data Protection Supervisor (EDPS) in 2020 on Europol's processing of large datasets.[624] The EDPS Decision focussed on Europol's analysis tasks performed on the Computer Forensic Network (CFN) under Art. 18(2)(b) and (c) Europol Regulation and identified risks of structural non-compliance by Europol. For the purposes of a big data analysis, Europol was prohibited from processing personal data beyond the categories of data subjects (suspects, potential future criminals, contacts and associates, victims, witnesses and informants of criminal activities).[625] Upon receiving large datasets, however, it is not possible for Europol, from the outset, to ascertain that all underlying information complies with the list of data subject categories. The EDPS Decision, therefore, inferred that Europol had processed personal data for which compliance with these requirements laid down in Europol Regulation for the purpose of (big) data analyses was uncertain and ascertained that this had occurred over a longer period of time resulting in conflict with the principle of *data minimisation*.[626]

The dilemma carved out by the EDPS Decision seemed rooted in functional necessity. On the one hand, Europol's handling of information for its (big) data analysis work[627] did not include activities to identify and segregate relevant data (including from large datasets received),[628] but had to commence on the basis of pre-sifted information containing only information of data subject categories of Annex II Europol Regulation (i.e. suspects, potential future criminals, contacts, associates, victims, witnesses and informants of criminal activities). On the other hand, the very nature of (big) data analysis by Europol had to include the process of minimising and aggregating information and data, by filtering and reducing the information contained in large datasets to what is relevant for operational support and the related investigations. To overcome this dilemma, Europol had issued a detailed Action Plan and, ultimately, called for a modification of the Europol Regulation in order to clarify and adjust the vital equilibrium between operational effectiveness and EU data protection standards.[629]

In January 2022, The EDPS notified Europol of its Order to delete data concerning individuals with no established link to a criminal activity (data lacking 'Subject Categorisation').[630] According to this EDPS Order requesting Europol to comply within 12 months, datasets older than 6 months which had neither undergone this Data Subject Categorisation, nor had been categorised as not belonging to permitted subject categories, had to be erased and Europol was no longer permitted to retain data about people who had not been linked to a crime or a criminal activity for long periods with no set deadline.[631]

---

[624] European Data Protection Supervisor (EDPS) Decision, D(2020) 2036, C(2019) 0370, 18 September 2020, available at: https://edps.europa.eu/sites/edp/files/publication/20-09-18_edps_decision_on_the_own_initiative_inquiry_on_europols_big_data_challenge_en.pdf.

[625] Art. 18(5) Europol Regulation (old) in connection with Annex II Europol Regulation (old).

[626] Art. 28(1)(c) Europol Regulation (old).

[627] Also beyond that for all operational processing purposes based on old Art. 18(5) in connection with Art. 18(2) Europol Regulation (old).

[628] Except for the possibilities provided for in Art. 18(6) Europol Regulation (old) to determine relevance for Europol's tasks.

[629] Europol, "Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge'", EDOC# 1131384 v 14A, 17 November 2020, page 2.

[630] „EDPS Decision on the retention by Europol of datasets lacking Data Subject Categorisation" in Cases 2019-0370 & 2021-0699, 21 December 2021, available at: https://edps.europa.eu/data-protection/our-work/publications/investigations/edps-orders-europol-erase-data-concerning_en.

[631] „EDPS Decision on the retention by Europol of datasets lacking Data Subject Categorisation" in Cases 2019-0370 & 2021-0699, 21 December 2021, p. 13.

- **New Data Protection Regime**

In June 2022, the Amending Europol Regulation modified the data protection regime of the Europol Regulation (new). The Amending Europol Regulation significantly expanded the mandate of Europol with regard to exchanges of personal data with private parties, the use of artificial intelligence, and the processing of large datasets. In addition, private parties have been added to the group of parties between which Europol may process personal data for the purpose of facilitating the exchange of information (Member States, Europol, other Union bodies, third countries, international organisations), Art. 18(2)(d) Europol Regulation (new). The new data protection regime aims at strengthening and in certain cases extending the mandate of Europol, in response to the changing security landscape and the evolving and increasingly complex threats.[632] In particular, the Amending Europol Regulation enables Europol to effectively support Member States and their investigations with the analysis of large and complex datasets, addressing the "big data challenge" for law enforcement authorities.[633]

In this regard, the Art. 18(6a) subparagraphs 1 and 2 Europol Regulation (new) require Europol to keep the personal data Europol has been provided with functionally separate and carry out a pre-analysis of for the sole purpose of determining whether such data falls into the categories of data subjects Europol is permitted to process. This pre-analysis has to take place within 6 months from the moment Europol ascertained that the received data fall within its objectives and any extension of this period has to be notified to the EDPS and is only possible to a maximum of 3 years, Art. 18(6a) subparagraph 2 Europol Regulation (new). Any data found in this pre-analysis as not in compliance with its objective, Europol has to delete (Art. 18(6a) subparagraph 3 Europol Regulation (new)), while it is required to make a clear distinction between the personal data that relate to the different categories of data subjects listed in Annex II, Art. 18(5a) Europol Regulation (new).

Data which do not relate to the categories of data subjects listed in Annex II of the Europol Regulation may only be processed by Europol in the two scenarios defined in the Art. 18a(1) Europol Regulation (new): (a) when a Member State, the EPPO or Eurojust provides investigative data to Europol and requests Europol to support that investigation either (i) by way of operational analysis or (ii) in exceptional and duly justified cases; (b) when Europol assesses that it is not possible to carry out an operational analysis or a cross-checking in support of that investigation without processing personal data that do not comply with the categories of data subjects listed in Annex II Europol Regulation. When either exception of Art. 18a(1) Europol Regulation (new) applies, the processing safeguards established in Art. 18a(2)-(5) Europol Regulation (new) regulate the storage, the operational analysis and the retention period of this data. However, both exceptions of Art. 18a(1) Europol Regulation (new) require an "ongoing specific criminal investigation". Similarly, the exception in Art. 18a(6) subparagraph 1 Europol Regulation (new) for datasets provided by third countries requires the data to be lawfully obtained "in the context of a criminal investigation" in addition to a "specific criminal investigation in one or more Member States".

From the perspective of the EDPS, the requirement of an "ongoing specific criminal investigations" has to be interpreted restrictively as referring only to specific cases which require the processing of large and complex

[632] Rec. (2) and (3) Amending Europol Regulation.
[633] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794 as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, COM/2020/796 final, 9 December 2020, page 3.

datasets, for which Europol is better placed to detect cross-border links.[634] If this requirement was not interpreted restrictively, then this would have considerable negative impact on the rights and freedoms of data subjects rendering Art. 18a Europol Regulation (new) effectively into a rule that trumps the logic of the principle of data categorisation governing the Europol Regulation.[635]

In the context of the GRACE project, the requirement of "specific criminal investigation" in Art. 18a(1) and (6) subparagraph 1 Europol Regulation (new) seems to prevent these exceptions to apply when considering CSEM reports referred to Europol by NCMEC, NCECC or the future EU Centre under the Draft Regulation Against Online CSA, because these three institutions are clearing houses referring the data of CSEM reports to Europol for the evaluation whether to initiate a criminal investigation in the first place.

Considering its previous "big data challenge" claim, the EDPS has shifted the focus on the transitional arrangements for the processing of personal data in Art. 74a and 74b Europol Regulation (new) according to which Member States may retroactively authorise Europol to process large data sets which had already been shared with Europol before the Amending Europol Regulation came into force. It will be interesting to see how the Court of Justice of the European Union (CJEU) will resolve EDPS's request to have Art. 74a and 74b Europol Regulation (new) annulled.[636] In the context of the GRACE project however, the previous "big data challenge" problem has been largely resolved by the Amending Europol Regulation because the GRACE tools and platform can only become available to LEAs after a potential roll-out in the future, whereas Art. 74a and 74b Europol Regulation (new) only impact Europol's personal data operations carried out in the past.

Concerning a potential future use of the GRACE tools and platform, Europol may use them as a rule only after the pre-analysis pursuant to Art. 18(6a) Europol Regulation (new) has identified the categories of personal data and data subjects Europol is permitted to process for the purposes of Art. 18(2)(a)-(d) Europol Regulation (new), unless either of the two narrow exceptions in Art. 18a(1) Europol Regulation (new) applies. However, the strict data protection safeguards set out in Art. 18a(1)-(4) Europol Regulation (new) also apply whenever LEA or international organisation of a third country provides investigative data to Europol for operational analysis that contributes to the specific criminal investigation in one or more Member States that Europol supports, Art. 18a(6) subparagraph 1 Europol Regulation (new).

As a general rule, requiring Europol to perform this pre-analysis pursuant to Art. 18(6a) Europol Regulation (new) in the interest of data protection appears as a functional necessity in the age of big data.

7.2.2.5. Draft Prüm II Regulation

As essential part of the Police Cooperation Code, the Draft Prüm II Regulation aims to facilitate automated

[634] EDPS, „Supervisory Opinion on Europol's Management Board Decisions adopted pursuant Art. 11(1)(q), 18 and 18a Europol Regulation" in Case 2022-0923, 17 November 2022, p. 9 at paras. 23 and 24; available at: https://edps.europa.eu/system/files/2023-01/22-11-17_edps_opinion_-_2022-0923_e-signed_en.pdf.
[635] EDPS, „12th Joint Parliamentary Scrutiny Group", Speech, 27 March 2023, p. 3, available at: https://edps.europa.eu/system/files/2023-03/23-03-27_speech_12_jpsg_en.pdf.
[636] EDPS, „EDPS takes legal action as new Europol Regulation puts rule of law and EDPS independence under threat", Press Release EDPS 2022/23, 22 September 2022, available at: https://edps.europa.eu/system/files/2022-09/EDPS-2022-23-EDPS-request%20to%20annul%20two%20new%20Europol%20provisions_EN.pdf.

data exchange between LEAs in different Member States and with Europol.[637] The main focus of the Draft Prüm II Regulation is to introduce facial images, police records and driving licence data as additional categories data eligible to automated comparison across the EU by establishing a new infrastructure for standardised procedures identifying a match of core data upon queries in individual investigations.

From a data protection perspective, it is interesting to note that both, Council's General Approach and Parliament's Draft Report seem to agree that the indication on whether a query concerns either "a suspect or a perpetrator of a criminal offence" would be insufficient as part of the minimum information to justify the processing of data by a national LEA or Europol in Art. 33(2)(b) Draft Prüm II Regulation. While the Council's General Approach suggests in this respect that a justification needs to indicate whether a query concerns "a suspect or a perpetrator of a criminal offence, a victim, a missing person or human remains",[638] Parliament's Draft Report appears to agree with this suggestion by the Council, but would only demand to limit the indication of "a victim" to victims either of a terrorist or a serious criminal offence as defined in Art. 4 (21) and (22) Regulation (EU) 2019/817.[639]

[637] Section 2.3.3 above provides an overview of the Draft Police Cooperation Code in general and the details of the Draft Prüm II Regulation in particular pointing out the deviating positions between the Commission, the Council and Parliament at the current stage of the legislative process.

[638] Art. 33(2)(b) in the General Approach of the Council on the Draft Prüm II Regulation, No. 9544/22, 31 May 2022, adopted on 10 June 2022, available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/10/council-adopts-recommendation-two-negotiating-mandates-improve-operational-police-cooperation-information-exchange/

[639] EU-Parliament, LIBE Committee, Draft Report on Draft Prüm II Regulation, 2021/0410(COD), 19 September 2022, Amendment 122, p. 60; available at: https://www.europarl.europa.eu/doceo/document/LIBE-PR-736469_EN.pdf.

8. Electronic Evidence

The production, dissemination, possession and accessing of CSEM is one of the most serious forms of victimisation of children and the online dimension of CSE is intrinsically tied to electronic data. Even though electronic data show unique characteristics that have a significant impact on their availability and admissibility as evidence, there is no comprehensive legal framework addressing these specific issues.

The GRACE project aims to develop effective investigative tools and a platform enabling law enforcement to investigate electronic data concerning CSE and CSEM as criminal evidence. Access to incriminating electronic evidence is crucial for LEAs in their fight against online CSE and entails two dimensions: The availability of electronic evidence for law enforcement depends on the type of electronic data, on the one hand, and on the data's location, on the other. Saving the dimension of LEAs' cross-border access to electronic evidence for a later deliverable, this section shed light on the lack of internationally uniform classification of electronic data as evidence in criminal investigations and proceedings.

After a general introduction to the key challenges for electronic data as criminal evidence this chapter takes a brief look at the most recent proposals aiming to overcome the lack of legal frameworks for electronic evidence in criminal investigations and proceedings in international treaties at global level by the United Nations (section 7.1. below) and at regional level by the Council of Europe (section 7.2. below) as well as at the proposal for electronic evidence within the European Union (section 7.3. below). Second, this chapter highlights an approach for classifying electronic evidence which has been developed by *Warken* based on the affected data subject's fundamental rights (section 7.4. below).

8.1. Challenges for Electronic Data as Criminal Evidence

While in the pre-computer age investigators were handling traditional types of evidence (such as documents and witnesses), the development and today widespread use of electronic devices has fundamentally changed the way LEAs work. With the focus on assisting LEAs in handling data-related CSEM investigations GRACE reflects this development and the relevance of electronic evidence.

The fundamental aim of GRACE is to provide LEAs with assistance – recognizing that LEAs need such guidance. While the project focuses on enabling LEAs to better scope with the quantitative challenges of increasing CSEM there are in addition significant additional challenges when handling electronic evidence. They range from a constantly evolving technical environment to the highly fragile nature of electronic evidence, that can so easily be deleted[640] or modified[641] that experts consider it alarming.[642] The burden of preventing such modification is on LEAs that have to act in an environment where loss or modification of data can in the worst scenario lead to wrongful conviction.[643]

---

[640] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.
[641] See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.
[642] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1,; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.
[643] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2,.

But even leaving those technical challenges of preserving the integrity of electronic evidence aside there are a number of – partly connected - legal issues that LEAs have to deal with. Despite a number of similarities between electronic evidence and other categories of evidence, there are major differences with legal significance. Some of the general principles[644], such as the requirement that the evidence be authentic, complete, reliable[645] and accurate and that the process of obtaining the evidence take place in line with the legal requirements, can successfully be applied to electronic evidence.[646] However, there are a number of aspects that make electronic evidence unique and therefore require special attention when dealing with electronic evidence in criminal investigations. There are especially a number of principles related to the admissibility of electronic evidence in court:

- The fundamental principle of *legitimacy* for example requires that electronic evidence has been collected, preserved and presented in court in accordance with the appropriate procedures and without violating the fundamental rights of the suspect.[647] Protecting integrity is necessary in order to ensure reliability and accuracy and to comply with the principle of legitimacy.[648] LEAs therefore need to make sure that evidence is not altered in any unauthorized manner during the investigation.[649]
- Another fundamental principle (particularly relevant for Common Law countries) is the *best evidence rule*.[650] Based on this principle only the best available evidence of a fact at issue is said to be admissible. While in the past the rule was of great importance, some express assertions of its demise.[651] With regard to electronic evidence, this raises a number of questions, insofar LEAs as well as courts have to determine what the best evidence is.[652] Electronic evidence can be copied without loss of quality and a presentation of the original data in court is not in all cases possible, the best evidence rule seems to be incompatible with electronic evidence. However, in recent years courts have started to open the rule to new developments by accepting an electronic copy as well as the original document.[653]
- According to the *rule against hearsay* (particularly relevant for Common Law countries) an assertion other than one made by a person while giving oral evidence in the proceedings and tendered as

[644] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 19.
[645] Regarding the liability of digital investigations, see: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.
[646] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161.
[647] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 207.
[648] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2,.
[649] *Menezes*, Handbook of Applied Cryptography, 1996, page 361.
[650] *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.
[651] Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332 and *Omychund v Barker* (1744) 1 Atk 21 at 49; *Robinson Bros (Brewers) Ltd v. Houghton and Chester-le-Street Assessment Committee* [1937] 2 KB 445 at 468, [1937] 2 All ER 298 at 307, CA, per Scott LJ.
[652] *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.
[653] With regard to different exemptions, see: *Nemeth*, Law of Evidence: A Primer for Criminal Justice, 2007, page 144 *et seq.*; Best Evidence Rule, California Law Review Commission, 1996, available at: www.clrc.ca.gov/pub/Printed-Reports/REC-BestEvidenceRule.pdf; *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

evidence of the facts asserted is inadmissible.[654] With regard to the fact that electronic evidence collected during an investigation in general intends to prove the truth of the matter asserted in the digital evidence itself, strict application of the rule is problematical in an age where very often electronic evidence is the most relevant category of evidence in court proceedings. In response, some Common Law countries have started to implement statutory exceptions to the hearsay rule.[655] Under these rules evidence produced by computers, cameras or other machines without incorporating any human statement cannot be rejected as hearsay.[656]

- Another principle is the one of *relevance*. In order to be admissible, various jurisdictions require evidence relevant and effective.[657] It can be challenging in investigations to ensure relevance and effectiveness if out of large quantities of data seized only small portions are actually relevant for an investigation. [658]

The challenge for GRACE and comparable approaches to develop solutions for LEAs that should be operated in various countries is that there is a lack of a harmonised legal framework dealing with electronic evidence and as a consequence a lack of clear rules and guidance with regard to the issues mentioned above. Only a few countries have so far addressed specific aspects of electronic evidence in a legal framework and, in addition, international binding standards are missing. The following assessment of as well as a review of differing national standards show a diverse legal environment. This limits the ability of GRACE to provide technical processes that by design comply with legal requirements as they may significantly differ.

8.2. Draft UN Convention on Cooperation in Combating Cybercrime

At the United Nations, there is no international treaty addressing a set of rules for the availability and admissibility of electronic data as evidence. However, Russia recently submitted a Draft UN Convention on Cooperation in Combating Cybercrime[659] and led a resolution[660] to establish a committee of experts to

[654] Per Lord Havers in *R v Sharp* [1988] 1 WLR 7 and per Lords Ackner and Oliver in R v Kearley [1992] 2 All ER 345 at 363 and 366 respectively. The rule also extends to out-of-court statements of otherwise admissible opinion.

[655] See in this context, for example, Part II of the Irish Criminal Evidence Act 1992.

[656] R v Dodson [1984] 1 WLR 971, 79 CrApp Rep 220, CA (photographic evidence); R v Maqsud Ali [1966] 1 QB 688, 49 Cr App Rep 230, CCA (tape recorded conversation); R v Wood (1982) 76 Cr App Rep 23, CA; Castle v Cross [1984] 1 WLR 1372, DPP v McKeown [1997] 1 All ER 737, 2 Cr App Rep 155, HL (computer evidence).

[657] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

[658] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

[659] See United Nations, General Assembly, Annex to the letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, A/C.3/72/12, 16 October 2017, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/329/59/PDF/N1732959.pdf?OpenElement.
from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General

[660] United Nations, Resolution 73/187, Countering the use of information and communications

consider establishing a UN cybercrime treaty. While the legitimacy of this Russian led UN resolution has raised suspicions,[661] the Association for Progressive Communication (APC) had previously argued in an open letter to the UN General Assembly that the Draft UN Convention on Cooperation in Combating Cybercrime proposed by Russia undermines the use of the internet to exercise human rights and facilitate social and economic development because: (i) this Draft opens the door to criminalising ordinary online behaviour; (ii) creates a chilling effect; (iii) this Draft lacks sufficient references to balancing the interests of law enforcement and respect for fundamental human rights are absent; and (iv) there is no need for a new international convention on cybercrime especially since a Second Additional Protocol is being developed to the CoE Budapest Convention[662] which is the most widely ratified international instrument on cybercrime.[663] Further, the establishment of an ad hoc intergovernmental committee of experts to address the issue of cybercrime would exclude key stakeholders who bring valuable expertise and perspectives both in terms of effectively countering the use of ICTs for criminal purposes and to ensure that such efforts do not undermine the use of ICTs for the enjoyment of human rights and social and economic development.[664]

The Draft UN Convention on Cooperation in Combating Cybercrime proposed by Russia distinguishes between computer data, subscriber information, traffic data and content data. While the term "computer data" is not explicitly defined, it seems to refer any data stored in an ICT device.[665] "subscriber information" is defined as any information held by a service provider relating to subscribers to its services other than traffic data or content data,[666] the term "traffic data" refers to any electronic information (other than its content) relating to the transfer of data.[667]

Update for Legal Report v2:

Pushing the Draft UN Convention on Cooperation in Combating Cybercrime proposed by Russia aside, the General Assembly decided to launch a process towards a new international treaty on cybercrime in December 2019 by establishing an open-ended ad hoc intergovernmental committee of experts (Ad Hoc Committee) to elaborate a "comprehensive international convention on countering the use of information and communications technologies for criminal purposes". [668] As also pointed out in section 2.1.1 above, the draft of a future UN convention on cybercrime is currently scheduled to be provided to the General Assembly at its

technologies for criminal purposes, General Assembly, A/RES/73/187, adopted on 17 December 2018, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/53/PDF/N1845053.pdf?OpenElement.

[661] Stolton, "UN backing of controversial cybercrime treaty raises suspicions", EURACTIV.com, 23 January 2020, available at: https://www.euractiv.com/section/digital/news/un-backing-of-controversial-cybercrime-treaty-raises-suspicions/.

[662] See section 6.3. of this Deliverable D9.3.

[663] APC, "Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online", 6 November 2019, available at: https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human.

[664] APC, "Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online", 6 November 2019, available at: https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human.

[665] Art. 26(1)(a) Draft UN Convention on Cooperation in Combating Cybercrime.

[666] Art. 25(3) Draft UN Convention on Cooperation in Combating Cybercrime.

[667] Art. 4(n) Draft UN Convention on Cooperation in Combating Cybercrime.

[668] General Assembly, „Countering the use of information and communications technologies for criminal purposes", Resolution 74.247, A/RES/74/247, adopted on 27 December 2019, p. 3 at para. 2, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement.

78th session, which will begin in September 2023 and conclude in September 2024.[669]

The Ad Hoc Committee's drafting process towards a future UN convention on cybercrime is intended to take into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes and, in particular, "the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime" (Expert Group).[670] However, it is important to note that the Ad Hoc Committee is a subsidiary body of the General Assembly and as such not only separate, but due to its different mandate also independent from the Expert Group which is a subsidiary body of CCPCJ, even though UNODC (another subsidiary body of CCPCJ) serves as Secretariat for the Ad Hoc Committee.[671]

The next step for the Ad Hoc Committee is to convene at least six negotiating sessions of 10 days each, held no less than 11 weeks apart; and held its first five negotiation sessions in March 2022[672], June 2022[673], September 2022[674], January 2023[675], and April 2023[676]. The sixth session in January 2024 is supposed to finalise the draft that will be concluded in a last session in January 2024.[677]

A challenge for all sessions is that all Ad Hoc Committee's decisions on substantive matters without approval

---

[669] General Assembly, „Countering the use of information and communications technologies for criminal purposes", Resolution 75.282, A/RES/75/282, adopted on 26 May 2021, p. 2 at para. 4, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement.
[670] General Assembly, Resolution 74.247, A/RES/74/247, adopted on 27 December 2019, p. 3 at para. 2; General Assembly, Resolution 75.282, A/RES/75/282, adopted on 26 May 2021, p. 2 at para. 11.
[671] General Assembly, Resolution 75.282, A/RES/75/282, adopted on 26 May 2021, p. 2 at para. 2.
[672] Ad Hoc Committee, Report of First Session, A/AC.291/7, 24 March 2022, available at: https://www.undocs.org/A/AC.291/7. All Documentation of the „First session of the Ad Hoc Committee" in New York, 28 February to 11 March 2022, is available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.
[673] Ad Hoc Committee, Report of Second Session, A/AC.291/10, 27 June 2022, available at: https://www.undocs.org/A/AC.291/10. All documentation of the „Second session of the Ad Hoc Committee", in Vienna, 30 May to 10 June 2022, is available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.
[674] Ad Hoc Committee, Report of Third Session, A/AC.291/14, 28 September 2022, available at: https://www.undocs.org/A/AC.291/14. All Documentation of the „Third session of the Ad Hoc Committee", in New York, 29 August to 9 September 2022, is available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_third_session/main.html.
[675] Ad Hoc Committee, Report of Fourth Session, A/AC.291/17, 2 February 2023, available at: https://www.undocs.org/A/AC.291/17. All Documentation of the „Fourth session of the Ad Hoc Committee", in Vienna, 9 – 20 January 2023, available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html.
[676] Documentation of the „Fifth session of the Ad Hoc Committee", in Vienna, 11 – 21 April 2023, available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main. The documentation also includes a „ Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes", A/AC.291/19, 19 December 2022, available at: https://www.undocs.org/A/AC.291/19.
[677] See: documentation of the „First session of the Ad Hoc Committee", 28 February to 11 March 2022, available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.

by consensus will be taken by a two-thirds majority of the representatives present and voting.[678] Meanwhile, the Ad Hoc Committee has already gone through its 5th session of negotiations in April 2023 and has developed a draft that is not yet fully complete.[679] In reviewing the draft, it becomes clear that the UN Convention is modelled on the CoE Convention on Cybercrime in broad and central areas.[680] For example, the scope and procedural measures in Art. 23 are taken from Article 14 of the CoE Convention. The general principles on international cooperation (Art. 46 ff.) are also based on Art. 23 of the CoE Convention on Cybercrime and Art. 43 of the Convention against Corruption (UNCAC). Other potentially relevant provisions on the retention of computer data (Art. 25) are borrowed from Art. 16 of the CoE Convention. Art. 11 deals with computer-related forgery and Art. 12 with computer-related theft and fraud, which in turn are modelled on Art. 7 and Art. 8 of the CoE Convention on cybercrime. In addition to the CoE Convention, the UN Convention is also modelled on existing UN conventions such as the Convention against Corruption (UNCAC), the Convention against Transnational Organized Crime (UNTOC), the Convention on the Rights of the Child, and the CoE Lanzarote Convention. The influence of Russia, which as mentioned above started the ball rolling for a UN convention on cybercrime, seems to have diminished in the course of the negotiations.[681] The European Commission, which has so far promoted the CoE Convention as an international standard in fighting cybercrime, has been authorised by Council Decision, with the aim of a consistent European and international legal situation, to participate intensively on behalf of the EU in the negotiations on the UN convention.[682] The negotiation directives for the European Commission are listed in a separate Addendum and a special committee has been designated by the Council.[683] Probably the inclusion of the EU is the reason why the UN Convention seems to be modelled on the CoE Convention on cybercrime in many areas. In its cooperation, the EU has in mind the protection of personal data and the fundamental right of individuals to respect for their private and family life, their home and their communications.[684]

Against this background, it remains interesting to see how the deadlock between opposing schools of thought will ultimately be resolved.

---

[678] General Assembly, Resolution 75.282, A/RES/75/282, adopted on 26 May 2021, p. 2 at para. 5.
[679] Draft text of the convention: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf.
[680] See: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/general-documents/AHC_6th_session_-_Explanatory_notes_on_DTC.pdf.
[681] Bannelier, The U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights, January 2023.
[682] Council Decision (EU) 2022/895 of 24 May 2022 authorising the opening of negotiations on behalf of the European Union for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, 8 June 2022, Official Journal of the EU L 155, p. 42, available at: https://op.europa.eu/en/publication-detail/-/publication/f701f8d8-e6c5-11ec-a534-01aa75ed71a1/language-en/format-PDF; the original recommendation by the Commission of 29 March 2022 for this Council Decision is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0132.
[683] Art. 2 in conjunction with the Addendum of Council Decision (EU) 2022/895, available at: https://op.europa.eu/en/publication-detail/-/publication/f701f8d8-e6c5-11ec-a534-01aa75ed71a1/language-en/format-PDF; Annex to the Recommandation for a Council Decision; available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0132.
[684] Explanatory Memorandum to the Recommendation for a Council Decision; available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0132.

8.3. Draft 2nd Additional Protocol to CoE Budapest Convention

The CoE Convention on Cybercrime establishes international mechanisms for cooperation against cybercrime and requires States Parties to establish powers and procedures to obtain electronic evidence and to provide each other mutual legal assistance. The electronic evidence is distinguished into computer data, traffic data and subscriber information. The term "computer data" refers to any representation of facts, information or concepts in a form suitable for processing in a computer system,[685] whereas "traffic data" means any computer data relating to a communication by means of a computer system.[686] In contrast, the term "subscriber data" means any information held by a service provider relating to subscribers of its services other than traffic or content data.[687]

With the aim of moving away from data storage location as a decisive factor, the Cybercrime Convention Committee (T-CY) is in the process of preparing a Second Additional Protocol[688] to the CoE Convention on Cybercrime which addresses the challenges to criminal justice in cyberspace and provides for more effective cooperation on electronic evidence. Art. 3(1) Draft Second Additional Protocol incorporates the definitions provided in the CoE Convention on Cybercrime for "computer data", "traffic data" and "subscriber information". At the beginning of May 2021, an additional stakeholder consultation has closed and it is expected that the Second Additional Protocol can be finalised and adopted in the course of 2021.[689]

Update Legal Report v2:

The Second Additional Protocol was opened for signature and signed by 22 State Parties[690] in May 2022 after which 14 more State Parties[691] have signed. Pursuant to Art. 16(3) Second Additional Protocol, five State Parties have to ratify the Second Additional Protocol for it to enter into force in the month following the last ratification. So far, Serbia is the only State Party having ratified the Second Additional Protocol in February 2023.[692]

---

[685] Art. 1(b) CoE Convention on Cybercrime.
[686] Art. 1(d) CoE Convention on Cybercrime.
[687] Art. 18(3) CoE Convention on Cybercrime.
[688] CoE, Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Draft Protocol version 2, 12 April 2021.
[689] CoE, „Towards a Protocol to the Convention on Cybercrime: additional stakeholder consultations", T-CY News, 14 April 2021, available at: https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultatio-1.
[690] The following 22 State Parties signed the Second Additional Protocol on 12 May 2022: Austria, Belgium, Bulgaria, Chile, Colombia, Estonia, Finland, Iceland, Italy, Japan, Lithuania, Luxembourg, Montenegro, Morocco, Netherlands, North Macedonia, Portugal, Romania, Serbia, Spain, Sweden and the United States of America.
[691] These 14 further signatories are: Andorra on 20 May 2022; Costa Rica on 13 June 2022; Croatia, Moldovia, Slovenia, Sri Lanka, Ukraine and the United Kingdom on 30 November 2022; Greece on 20 January 2023; France and Germany on 27 January 2023; Dominican Republic on 30 January 2023; Argentina on 16 February 2023; and Albania on 27 February 2023. See also sections 2.2.5 and in 7.1.2.3. above.
[692] According to the chart of signatures and ratifications of Treaty CETS No. 224, Serbia ratified the Second Additional Protocol on 9 February 2023: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 (last accessed on 26 March 2023).

8.4. Proposal for EU-Regulation on Electronic Evidence

In April 2018, the European Commission presented a legislative package on electronic evidence consisting of a proposal for a Regulation on European Production and Preservation Orders in criminal matters[693] and a proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[694] The proposed Regulation has entered the trilogue stage of the legislative process on 10 February 2021[695] and aims to introduce binding European Production and Preservation Orders which can be issued to seek preservation or production of data that are stored by a service provider located in another jurisdiction and that are necessary as evidence in criminal investigations or criminal proceedings.[696]

The categories of data that can be obtained with a European Production Order by the competent authorities include "subscriber data", "access data", "transactional data" (the three categories commonly referred to jointly as '*non-content data*') and stored *content data*. This distinction, apart from the access data, exists in the legal orders of many Member States and also in non-EU legal frameworks.[697] According to Art. 2(6) Draft Regulation on Electronic Evidence in Criminal Matters, 'electronic evidence' means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored *subscriber data*, *access data*, *transactional data* and *content data*. The term *"subscriber data"* means any data pertaining to the identity of a subscriber and to the type of service and its duration.[698] The term *"access data"* refers to data related to the commencement and termination of a user access session to a service.[699] The term *"transactional data"* means data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and includes metadata.[700] Finally, the term *"content data"* refers to any stored data in a digital format such as text, voice, videos, images, and sound.[701]

Because the legislative process of the Regulation and of the Directive is still pending, the current EU legal framework consists of Union cooperation instruments in criminal matters, such as the Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO Directive)[702] and the Convention on

[693] Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17 April 2018.
[694] Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings
[695] See Council of the EU, "E-Evidence Package: First Trilogue Meeting", 10 February 2021, available at: https://www.2021portugal.eu/en/news/e-evidence-package-first-trilogue-meeting/.
[696] Commission, Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17 April 2018, p. 4.
[697] Commission, Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17 April 2018, p. 14.
[698] Art. 2(7) Draft Regulation on Electronic Evidence in Criminal Matters.
[699] Art. 2(8) Draft Regulation on Electronic Evidence in Criminal Matters.
[700] Art. 2(9) Draft Regulation on Electronic Evidence in Criminal Matters.
[701] Art. 2(10) Draft Regulation on Electronic Evidence in Criminal Matters.
[702] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, 1 May 2014, Official Journal of the EU L 130, p.1.

Mutual Assistance in Criminal Matters between the Member States of the European Union.[703] Referring to national Member State law, the EIO Directive itself neither defines the term evidence nor distinguishes different types of data.

Update Legal Report v2:

In January 2023, the final compromise texts for both, the eEvidence Directive as well as for the eEvidence Regulation were agreed upon. While the Council of the EU has already confirmed this agreement on the final texts,[704] the final text versions currently still await formal legislative approval. This section provides a brief overview of relevant changes in the final compromise texts.[705]

In the final compromise text of the eEvicence Regulation[706], the categories of data that can be obtained with a European Production Order by the competent authorities have been renamed into *"subscriber data"*, *"data requested for the sole purpose of identifying the user"* and *"traffic data"* (the three categories commonly referred to jointly as '*non-content data*') and stored *content data*. Accordingly, the definition of *"electronic evidence"* in Art. 2(6) eEvidence Regulation refers to *subscriber data*, *traffic data* or *content data* stored by or on behalf of a service provider, in an electronic form, at the time of receipt of a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR). The term *"subscriber data"* has been specified as to mean any data held by a service provider relating to the subscription to the services, pertaining to the identity of a subscriber and to the type of service and its duration.[707] The term "*traffic data*" has been newly introduced and refers to data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and includes metadata.[708] The term *"content data"* has remained unchanged and still means any data in a digital format such as text, voice, videos, images, and sound.[709] In addition, the term *"data requested for the sole purpose of identifying the user"* has been introduced and refers IP addresses as well as the relevant source ports and time stamp (date/time), or technical equivalents of these identifiers and related information where requested by LEAs for the sole purpose of identifying the user in a specific criminal investigation.[710]

---

[703] Council Act of 29 May 2000 establishing in accordance with Article 34 TEU the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU, 12 July 2000, Official Journal of the EC, 43 C 197, p. 1.

[704] Council of the EU, „Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence", Press Release 48/23, 25 January 2023, available at: https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/.

[705] See also section 2.3.2 above.

[706] Council of the EU, Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, final compromise text, 5448/23, 20 January 2023, available at: https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf.

[707] Art. 2(7) eEvidence Regulation.

[708] Art. 2(9) eEvidence Regulation. The Commission had proposed to term this kind of data "transactional data", Art. 2(9) Draft eEvidence Regulation.

[709] Art. 2(10) eEvidence Regulation.

[710] Art. 2(8) eEvidence Regulation. The term *"data requested for the sole purpose of identifying the user"* has evolved in the course of the legislative process. The Commission had originally proposed in Art. 2(8)

In the context of cybercrime investigations, it is important to point out that the final compromise text of the eEvidence Directive[711] envisions to introduce an obligation for OSPs to appoint a legal representative in the EU Member State where it is established or with which the OSP has a "substantial connection".[712] According to Recital 13 eEvidence Directive a "substantial connection" means that (a) the OSP enables legal or natural persons in the EU to use its services, and (b) is established in in the EU or (c) there is a significant number of users of its services in one or more EU MS, or (d) it targets its activities towards one or more EU MS (for example based on the language it uses to promote its services, or on the currency allowed for transactions). Bearing in mind that neither Denmark nor Ireland participate in the judicial cooperation instruments adopted under Title V, Chapter 4, of the TFEU, leaving the choice of the EU Member State for legal representative to the OSP seems to risk effectiveness. However, the legal representative should be empowered by the OSP to respond to and execute the Preservation and Production Orders introduced by the eEvidence Regulation.

The final compromise text of the eEvidence Regulation envisions to introduce two new legal instruments for access to electronic evidence:

- The **European Production Order** aims at gaining access to *electronic evidence* (= *subscriber data*, *traffic data* or *content data*.[713]
- The **European Preservation Order** aims at preserving *electronic evidence* by freezing a set of data to avoid its loss.[714]

Both orders are served by competent authorities of an EU Member State[715] (depending on the category of data sought, different authorities may have competence) either to the *designated establishment*[716] or to the *legal representatives*[717] designated by the relevant OSP.[718]

Taken together, the eEvidence Regulation and the eEvidence Directive (eEvidence Package) offer several improvements for future cybercrime investigations. *First*, by moving away from considering data location as a determining connecting factor and preferring the economic presence, the eEvidence Package has the potential to overcome key challenges encountered currently in establishing jurisdiction, and proves to be fit for modern technologies such as the cloud, which transcend traditional territorial borders. *Second*, the eEvidence Package creates a direct link with the OSP, thus avoiding the additional step of traditional MLA procedures where the judicial authority of the foreign country needs to be involved. This potentially shortens the overall timeframe, as well as the administrative burden. *Third*, the eEvidence Package creates a mandatory framework,

Draft eEvidence Regulation to define a term *"access data"* as referring to data related to the commencement and termination of a user access session to a service.

[711] Council of the EU, Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, final compromise text, 5449/23, 20 January 2023, available at: https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/en/pdf.

[712] Art. 3(1) in conjunction with Art. 2(3) eEvidence Directive.

[713] Art. 2(1) eEvidence Regulation.

[714] Art. 2(2) eEvidence Regulation.

[715] Art. 4 eEvidence Regulation.

[716] Defined in Art. 2(5a) eEvidence Regulation.

[717] Defined in Art. 2(5b) eEvidence Regulation.

[718] Art. 7(1) eEvidence Regulation.

introducing short deadlines[719], enforcement mechanisms[720] and sanctions[721] for non-compliance. *Finally*, the eEvidence package includes five clear and user-friendly forms in its annexes,[722] thus standardising the channels for cooperation.

8.5. Rights-Oriented Approach Classifying Electronic Evidence

There is a wide range of potential interference with fundamental rights through the acquisition and the use of electronic data in a criminal investigation. This broad range of potential intrusiveness calls for a set of possible measures with different conditions and safeguards. Consequently, differentiating electronic data seems an indispensable requirement for any comprehensive legal framework.

As seen in the lack of international treaties as well as in the proposed EU rules above, different levels of sensitivity are assumed only regarding communication data distinguishing between *content data* and *non-content data* (or metadata), while *non-content data* are further broken down into *subscriber data* and *traffic data*. This differentiation derives from the transition of classical telecommunication providers from analogue to digital networks in the early 1990s when, for billing purposes, the companies had to rely on the data provided in the service contract and provide traffic data as proof for the use of the service. In this scenario, the content of a communication was of no relevance for the involved service provider.[723]

Today, the content of a communication can no longer automatically be assumed more sensitive than non-content data that the user does not want to share publicly. In exchange for a social media service, the user increasingly does not have to pay with money. Rather, the use of the social media service generates data including content data which represents a significant economic value for the service provider because this data can be used for tailored advertising.[724] Because the traditional model of classifying electronic data seems to have served its time, a comprehensive and technologically neutral approach for determining the criteria for a dataset's sensitivity has been focused on the fundamental rights of the data subject. The specific fundamental rights concerning electronic data encompass the right of respect for private life,[725] the right to data protection,[726] the right of self-determination, and the right of secrecy of correspondence. The key content of the relevant fundamental rights regarding electronic data is the data subject's possibility to freely and independently decide what happens to his/her data and who has access to this data. Thus, the core issue of

[719] 10 days, pursuant Art. 9(1) eEvidence Regulation, which become 8 hours in cases of emergency or 96 hours after a mandatory prior notification Art. 9(2) eEvidence Regulation.
[720] Art 14 eEvidence Regulation. In comparison, the EU-US MLAT will only include enforceable mechanisms when the executive agreement under the Cloud Act is signed. The CoE Convention on Cybercrime will become mandatory only once its Second Additional Protocol is signed by all Parties.
[721] Art. 13 eEvidence Regulation.
[722] The five forms are: the "European Production Order Certificate (EPOC) for the production of electronic evidence" in Annex I; the "European Preservation Order Certificate (EPOC-PR) for the preservation of electronic evidence" in Annex II, the "Information on the impossibility to execute the EPOC / EPOC-PR" in Annex III, the "Confirmation of Issuance of request for production following a European Preservation Order" in Annex IV and the "Extension of the preservation of electronic evidence" in Annex V of the eEvidence Regulation.
[723] Warken, „Classification of Electronic Data for Criminal Law Purposes", eucrim 4/2018, p. 226 (at p. 228).
[724] Becker, „Consent Mangement Platforms und Targeted Advertising zwischen DSGVO und ePrivacy-Gesetzgebung", CR 2021, pp. 87–98.
[725] Art. 7 EU Charter of Fundamental Rights.
[726] Art. 8 EU Charter of Fundamental Rights.

data-related fundamental rights relates to the confidentiality of the data.[727]

Relying solely on the criterion of the data subject's reasonable expectation of confidentiality, the following five data categories have been convincingly suggested as more granular, but workable classification of electronic data (in order of decreasing sensitivity): (i) data of core significance for private life, (ii) secret data, (iii) shared confidential data, (iv) data of limited accessibility, and (v) data of unlimited accessibility.[728] This approach for classifying electronic data has the advantage of coherence with the existing classifications of other types of criminal evidence, e.g. documents or body-related information, both of which are also categorised according to the level of interference with the affected fundamental rights.[729]

[727] Warken, „Classification of Electronic Data for Criminal Law Purposes", eucrim 4/2018, p. 226 (at p. 229).
[728] Warken, „Classification of Electronic Data for Criminal Law Purposes", eucrim 4/2018, p. 226 (at p. 229).
[729] Warken, „Classification of Electronic Data for Criminal Law Purposes", eucrim 4/2018, p. 226 (at p. 232).

9. Legislation Related to CSEM Databases

In this project techniques in machine learning to the referral and analysis elaboration are used to fight the distribution of CSEM. The GRACE Consortium will use resources of EUROPOL and its nine Member State LEAs to provide early, frequent and flexible results that will be handed back to EUROPOL and Member State LEAs, helping to ensure their future technological autonomy.

The use of databases related to CSEM is a key component of the GRACE project. While the country reports (sections 10.–14. below) in this Deliverable underline their great practical relevance and value, until today there is no specific legislation on European level that either harmonises the legal framework related to such databases throughout the Member States, or creates a centralised European Database.

While the European Commission has undertaken important steps harmonising the criminal legislation related to CSEM, the position related to databases has remained largely unchanged for the last 20 years. In 2003, the European Commission responded to the question "what action can be taken in order to put a stop to such activities" ("on-line child pornography and paedophilia") that the Commission felt not competent for the process of actually setting up a database. It stated: "This is left to the appreciation of the EU Member States and other countries wishing to participate."[730]

9.1. Databases

Though not focus of this chapter it should be underlined that there are various databases related to CSEM:

- EU Member States: In fact, several Member States have built up their own national databases with CSEM (photographs, films, videos, magazines, picture and video files). In Germany, for example, the "Central Office for Combatting Sexual Offences Against Children and Adolescents"[731] was established at the Federal Criminal Police Office (BKA) in 1995 in order to evaluate CSEM content and the "Hash-Datenbank Pornografische Schriften (HashDBPS)" is maintained.[732]
- USA: The National Centre for Missing and Exploited Children (NCMEC) in the United States runs a National database, called CSAM (Child Sexual Abuse Material).
- Interpol manages the ICSE (International Child Sexual Exploitation) database. This database holds more than 2,7 million images and videos and has helped to identify 23.500 victims worldwide.[733] The EU Member State LEAs are able to use this database both in the course of their own investigations and to pass on related national information. The access to this database takes place within the collaboration with EUROPOL and INTERPOL. Even States that want to be become members of the EU are welcome to cooperate with EUROPOL. Using image and video comparison software, investigators are instantly able to make connections between victims, abusers, objects and places. The database

[730] Written Question E-1468/03 by Cristiana Muscardini (UEN) to the Commission (30 April 2003).

[731] Zentralstelle für die Bekämpfung von Sexualdelikten zum Nachteil von Kindern und Jugendlichen, BKA: https://www.bka.de/DE/UnsereAufgaben/Aufgabenbereiche/Zentralstellen/Kinderpornografie/kinderpornografie_node.html.

[732] Bericht der Stabsstelle: Revision der kriminalpolizeilichen Bearbeitung von sexuellem Missbrauch an Kindern und Kinderpornografie, Ministerium des Inneren NRW, 2020.

[733] Data about the Interpol database are available at: www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

avoids duplication of efforts and saves precious time by letting investigators know whether a series of images has already been discovered or identified in another country, or whether it has similar features to other images.[734]

9.2. Legislation

The most important guidance for the Member States in their fight against CSEM is the EU Directive 2011/93/EU on the sexual abuse and sexual exploitation of children and child pornography.[735] This Directive refers to the UN Convention on the Rights of the Child as well as the CoE Lanzarote Convention.[736] While all three documents create important legal frameworks with regard to the protection of children and the fight against CSEM, none of the documents contains concrete measures related to databases. Even the CoE Convention on Cybercrime[737] that specifically addresses Cybercrime and in this context CSEM, gives no indications for creating an (international) database to fight child exploitation.

9.3. Resulting Fragmentation

The European Commission does not get tired to underline the importance of fighting child sexual exploitation – most recently in the EU Strategy for a fight against child sexual abuse: "The fight against child sexual abuse is a priority for the EU. The European Parliament and the Council have both called for further concrete action. Similar calls have been made globally in multiple forums, including by the media, as it has become evident that the world as a whole is losing the battle against these crimes, and is failing to effectively protect the right of each child to live free from violence. The EU therefore needs to reassess and strengthen its efforts …"[738] However, this has so far not materialised in efforts to implement a harmonised legal framework for national CSEM databases or for establishing a centralised EU database. The consequence for GRACE is, therefore, that the utilisation of such databases cannot be based on rules extracted from a harmonised international/regional framework. Rather, the rules and regulations regarding the use of databases for CSEM remain fragmented into national entities.

[734] Available at: www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

[735] Directive 2011/93/EU of the European Parliament and the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[736] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS No. 201.

[737] Council of Europe Convention on Cybercrime, ETS No. 185.

[738] Communication from the Commission to the European Parliament, the Council, the European economic and social Committee of the Regions, EU strategy for a more effective fight against child sexual abuse, COM (2020) 607.

Update Legal Report v2:

9.4. Draft Regulation Against Online CSA

With the proposal of the Draft Regulation Against Online CSA[739] in May 2022, the European Commission has taken on the challenge to establish centralised EU databases for CSA material. In fact, the Draft Regulation Against Online CSA aims for no less than four different databases created, maintained and operated by the EU Centre concerning CSA material:

- *First*, the EU Centre is mandated to operate a *database for all the CSA reports* submitted to it by providers, Art. 45(1) Draft Regulation Against CSA. This database is intended to contain not only each individual CSA report[740], but also detailed information about the EU Centre's assessment and the exact further handling of each CSA report[741] as well as the *relevant indicators* and ancillary tags associated with the reported potential CSA material.[742]
- *Second*, the EU Centre is mandated operate a *database of indicators* to detect *known* CSA material, Art. 44(1)(a) Draft Regulation Against Online CSA.
- *Third*, the EU Centre is mandated to operate a *database of indicators* to detect *unknown* CSA material, Art. 44(1)(b) Draft Regulation Against Online CSA.
- *Fourth*, the EU Centre is mandated to operate a *database of indicators* to detect the *solicitation of children*, Art. 44(1)(c) Draft Regulation Against Online CSA.

Access to all four databases is controlled by the EU Centre and governed by Art. 46 Draft Regulation Against Online CSA. The *database of CSA reports* may only be accessed by Europol when assisting investigations of suspected CSA offences.[743] In contrast, access to the three *databases of indicators* is open not only to Europol but also to LEAs, the Coordinating Authorities and providers: While Europol and LEAs may access the *databases of indicators* for investigating suspected CSA offences,[744] the national Coordination Authorities may access the *databases of indicators* for the performance of their tasks including their investigatory powers,[745] but providers may access the *databases of indicators* only for the execution of a detection or blocking order.[746]

The reason for the wider accessibility of the *databases of indicators* is operational. may solely contain the *relevant indicators* and the necessary additional information facilitating their use[747]. These databases contain *relevant indicators* which are digital identifiers for the detection of known or new CSA material or the solicitation of children[748] including URLs of known CSA material[749].

[739] Section 4. above provides a detailed overview of the Draft Regulation Against Online CSA.
[740] Art. 45(2)(a) Draft Regulation Against Online CSA.
[741] Art. 45(2)(b)-(f) Draft Regulation Against Online CSA.
[742] Art. 45(2)(g) Draft Regulation Against Online CSA.
[743] Art. 46(5) Draft Regulation Against Online CSA.
[744] Art. 46(4) Draft Regulation Against Online CSA.
[745] Art. 46(3) Draft Regulation Against Online CSA.
[746] Art. 46(2) Draft Regulation Against Online CSA.
[747] Art. 44(2)(c) Draft Regulation Against Online CSA.
[748] Art. 44(2)(a) Draft Regulation Against Online CSA.
[749] Art. 44(2)(b) Draft Regulation Against Online CSA.

9.5. Draft Prüm II Regulation

Art. 43 Draft Prüm II Regulation regulates queries to national databases via *European Police Records Index System* (EPRIS).

10. Use of Crawler

One potential features of the GRACE solution will be targeted crawlers that are used for data acquisition.[750] Unlike traditional web crawlers[751] that create an index of available content, the tool utilized within the GRACE solution will focus on enriching existing data sets with additional information.

10.1. Lack of International/European Legal Framework

As highlighted by legal analysis carried out as part of other H2020-funded projects, such as TENSOR[752], there is no comprehensive legal framework addressing the use of crawlers by LEAs. There is not even a single specific provision addressing this issue. Therefore, for the legal evaluation of a LEA's authorization to use crawlers as intended by the GRACE solution, the general legal framework applies. The following sections provide an overview about some of the most relevant areas of law potentially triggered.

10.2. Data Protection

These days data protection has become a major issue in Europe. With the General Data Protection Regulation (GDPR) a harmonized framework has successfully been introduced.[753] While the GDPR provides answers to many pressing questions, the continuing development of new technologies – especially with regard to collection of information – keeps raising manifold new questions related to data protection.

As explained further in Chapter 5. above that specifically addresses data protection issues, the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) TFEU clearly point out that everyone has the right to the protection of personal data concerning themselves. Any processing of personal data, therefore, must be in compliance with the principles and rules stipulated in the GDPR as well as in compliance with the relevant supplementing national data protection legislation.

When it comes to the automatic collection of intelligence through a web crawler the discussion about data protection is of great relevance as the data collected may in general include personal data. This may lead to potential legal issues unless counter-measures are implemented that are aiming to avoid the unintentional collection of such personal data. But even if such measures are implemented (preferably already by-design) this is unlikely to eliminate the risk of personal data being processed entirely as it will be challenging to

[750] See 1.4.1.2 GRACE Grant Agreement

[751] Regarding the fundamental concepts and functions of web crawling see: *Olston/Najork*, Web Crawling, 2010.

[752] Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition, Grant Agreement ID: 700024, Sept. 2016 to Nov. 2019.

[753] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); For a general introduction see: *Voigt/von dem Bussche*, The EU General Data Protection Regulation, 2017

differentiate at the time of collection what data qualifies as personal data and as such is covered by data protection legislation and which data is not. In addition, content filtering requires deep packet inspection, which by itself is extremely intrusive from the point of view of privacy and data protection.[754]

10.3. Illegal Content – Other Than CSEM – Terrorist Content

One general area of concern regarding automated searches is that it could lead to the collection of illegal content. With regard to some types of illegal content – namely CSEM – the mere possession is illegal and could, therefore, lead to criminal investigations against the operator of the crawler. Within the GRACE project, this risk seems less relevant as the crawler is utilized in the context of CSEM investigations and by authorized LEAs.

However, there are potential concerns with regard to other categories of illegal content such as violent extremism and terrorism. It should be pointed out that the degree of criminalization and, therefore, the potential concerns related the accidental collection of the text and audio-visual material containing violent extremisms and terrorism is not equivalent to the level regarding CSEM (in which case the mere possession in many jurisdictions is a crime). It is also true that some countries have implemented legislation criminalizing the exchange of terrorist content. One example for such criminalization is Art. 578 of the Spanish Criminal Code. In addition, some countries are at this moment discussing to implement criminal sanctions for the possession of certain terrorist content.[755]

10.4. Circumventing Access Restrictions

One function frequently discussed in the context of automated crawlers is the ability to circumvent access restriction measures that de-facto prevent crawlers from accessing certain content. Of course, the question whether the circumvention of access restrictions may violate statutory law will only be relevant, if the crawler was equipped with such technology. Both the 2001 CoE Convention on Cybercrime[756] as well as the 2013 EU Directive on attacks against information systems[757] include provisions criminalizing such illegal access. If the operation of a crawler was, however, limited to publicly available information that are not protected by access restrictions, this discussion is less relevant. Based on the current status of the vision for the GRACE solution the intended crawler will not have capabilities to circumvent access restrictions.

10.5. Copyright

If the potential GRACE crawler is designed in a way that it collects large quantities of content, such collection process could go along with risks related to copyright violations. The web-crawler might copy and save content in a database that is protected by copyright laws. This issue is among the most frequently discussed legal issues

[754] *Porcedda*,, Data Protection and the Prevention of Cybercrime: The EU as an area of security?, 2012, available at: http://cadmus.eui.eu/handle/1814/23296

[755] See for example: *Evans*, Government considers new law to ban the possession of terrorist propaganda, The Telegraph, 14.01.2020.

[756] Council of Europe, Convention on Cybercrime, ETS 185.

[757] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

related to web-crawlers (especially those used by search engines).[758] And it would be too easy to take the position that it can hardly be illegal for a research project to do what search engines do on a daily basis as in some countries search engines operate on the basis of specific legislation that exempts them from liability that is not applicable to LEAs and researchers. The EU E-Commerce Directive[759] does not contain standards defining the liability of search-engine operators. However, some EU Member States have decided to address the liability of search-engine providers in a dedicated provision.[760] But it is important to point out that like in the case of hyperlinks, not all countries have based their regulation on the same principles.[761] Spain[762] and Portugal have for example based their regulations regarding the liability of search-engine operators on Article 14 of the E-Commerce Directive, while Austria[763] has based the limitation of liability on Article 12 E-

[758] See in this regard for example: *Rotenberg/Compano*, Search Engines for Audio-Visual Content: Copyright Law and its Policy Relevance, published in Preissl et al., Telecommunication Markets, 2009.

[759] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[760] Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

[761] See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

[762] Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) – Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (Spain)

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No. tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere la letra a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado primero no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

[763] Ausschluss der Verantwortlichkeit bei Suchmaschinen

§ 14. (1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er

1. die Übermittlung der abgefragten Informationen nicht veranlasst,

2. den Empfänger der abgefragten Informationen nicht auswählt und

3. die abgefragten Informationen weder auswählt noch verändert.

Commerce Directive. As hinted at above, this framework cannot simply be transferred to crawlers utilized by LEAs and it is, therefore, not possible to refer to search engines operating web-crawlers when discussing the legal basis.

Update Legal Report v2:

The crawling tool incorporated in the GRACE system might copy and save content in a database that is protected by copyright laws. This issue is frequently discussed in the context web-crawlers used for web-scraping[764] or by search engines.[765] Search engines frequently use technology similar to the one most likely utilised for the crawling tool of the GRACE system. While the core function of a search engine is to create and maintain a search index for the internet in which searches can be performed based on user queries,[766] one typical auxiliary function offered by search engines is to archive entire copies of the indexed content and make them available via a link commonly termed "cache".[767]

The crawling tool to be integrated in the GRACE system to systematically search for content anywhere in the internet, especially in social media which may as Open Source Intelligence (OSINT) help prioritise CSEM reports. This crawling tool would appear unlikely to produce sufficient results, if no copies of the searched content were retained at all. For the compliance of the crawling tool intended for the GRACE system therefore, a closer look at the requirements of copyright law appears appropriate. However, the requirements of copyright law are established at national level according to the Bern Convention.[768] Nevertheless, the Copyright Directive[769] and the Database Directive[770] have harmonised the compliance requirements to some extent.

10.5.1. Database Protection

For the applicability of the Database Directive, a social media platform has to constitute a database. A *database* is defined in Art. 1(2) Database Directive as a "collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means". On social media platforms, user posts are routinely arranged in chronological order and can be accessed individually. Furthermore, the set-up of social media platforms usually necessitates substantial

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

[764] Gausling, CR 2021, p. 609 (p. 613 at paras. 25 et seq.).
[765] Heßeling, Suchmaschinen im Konflikt mit dem Urheberrecht, 2014, p. 10.
[766] Sesing-Wagenpfeil, CR 2023, p. 113 (p. 114 et seq. at paras. 5 – 10).
[767] Sesing-Wagenpfeil, CR 2023, p. 113 (p. 116 at para. 14).
[768] Bern Convention for the Protection of Literary and Artistic Works, adopted in 1886, available as last amended on 28 September 1979 at: https://www.wipo.int/wipolex/en/treaties/textdetails/12214.
[769] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, Official Journal of the EU, 17 May 2019, L 130, p. 92, available at: https://eur-lex.europa.eu/eli/dir/2019/790/oj.
[770] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, as amended by teh Copyright Directive, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:01996L0009-20190606&from=EN.

investments as required in Art. 7(1) Database Directive, so that a social media platform regularly qualifies as a *database* under the Database Directive.

The protected right of the maker of a database is infringed when, according to Art. 7(2)(a) Database Directive, an unlawful *extraction* from a *database* occurs which requires not only a transfer of contents of a database to another medium by any means or in any form, but also that the transferred content constitutes either all or a substantial part of the database's content. The crawling tool integrated in the GRACE system would extract individual posts of a social media platform which match the search criteria for the enhancement of a CSEM report. If a social media platform was dedicated to posting CSEM and information concerning CSE, then the crawling tool could infringe the right of the maker of the database. In this context, it is also noteworthy that the Court of Justice of the European Union (CJEU) considered the use of a meta search tool as infringement of the sui generis right of the database maker.[771]

10.5.2. Copyright Protection

Art. 4(1) Copyright Directive provides that it is for the Member States to provide exceptions from copyright protection for text and data mining in national law. These exceptions in national law apply on condition that the use of the copyright-protected material has not been expressly reserved by their rightholders in an appropriate manner, such as machine-readable means in the case of content made publicly available online, Art. 4(3) Copyright Directive. As a result, even under the harmonised copyright framework for the EU there can still be national copyright law applicable in a Member State which the envisioned crawling tool incorporated in the GRACE system could infringe. The applicable compliance framework concerning copyright protection of searches can, therefore, only be evaluated for each Member State individually.

A further challenging condition for the lawfulness of the reproduction of copyrighted works by the use of a crawling tool is that, according to Art. 4(2) Copyright Directive such reproductions may only be retained for as long as is necessary for the purposes of text and data mining. Once a reproduction is no longer necessary for the purposes, national copyright law might require the deletion of the reproduction like in § 44b(2) sentence 2 of the German Copyright Act.[772]

10.6. Impact on Design Process

If the GRACE solution was to include a crawler with focus of data acquisition,[773] it is important that already at the stage of the design legal considerations are taken into consideration. Such considerations range from avoiding potential copyright and data protection violations to ensuring that if the crawler is equipped with

[771] CJEU, decision of 19 December 2013 in case C-202/12, ECLI:EU:C:2013:850, Innoweb v. Wegener, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=145914&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=291283.
[772] Müller-ter Jung/Rexin, CR 2022, p. 169 (p. 174 at paras. 32 and 33).
[773] See 1.4.1.2 GRACE Grant Agreement.

technology to circumvent access protections, the utilization of such technology does not constitute a criminal offence.

Update Legal Report v2:

10.7. Prohibition in Terms & Conditions

The use crawling tool for the GRACE system might also involve compliance risks related to the terms and conditions for the use of the websites which potentially contain content data collected as OSINT for the prioritisation of the CSEM reports provided by NCMEC, NCCECC and the future EU Centre. In this respect, it seems appropriate to look more closely at the scenario in which access to the desired content is only prohibited by the terms and conditions for the use of the website.

In the first scenario, access to the desired content is technologically possible, but explicitly prohibited for crawling tools by a website's terms and conditions. Many websites and especially social media platforms protect their own interests in their terms and conditions by explicitly excluding any kind of crawling tool from accessing their website and collecting data. The current Facebook Terms of Service for example, expressly state *"You may not access or collect data from our Products using automated means (without our prior permission) or attempt to access data you do not have permission to access. We also reserve all of our rights against text and data mining."*[774]

In the USA, Facebook has sued two companies which had engaged in an international "data scraping" operation gathering data from Facebook and Instagram users for "marketing intelligence" purposes.[775] More interestingly, at the heart of the landmark case *LinkedIn Corp. v. HiQ Labs, Inc.* is the question whether LinkedIn's terms and conditions for the use of its social media platform entitled LinkedIn to ban HiQ Labs from crawling and scraping content at LinkedIn. The LinkedIn User Agreement explicitly states as "Don'ts" that the user agrees to not "*develop, support or use software, devices, scripts, robots or any other means or processes (including crawlers, browser plugins and add-ons or any other technology) to scrape the Services or otherwise copy profiles and other data from the Services*" or to "*use bots or other automated methods to access the Services, add or download contacts, send or redirect messages*".[776] This case started in 2017 and has already escalated to the US Supreme Court[777] on the question whether HiQ Labs' access to LinkedIn's content violated the Computer Fraud and Abuse Act (CFAA) which was denied.[778] In November 2022, the District Court found

[774] See under no. "*3. Your Commitments and Our Community*" in subsection "*2. What you can share and do on Meta Products*" at para. 3 in Facebook Terms of Service, available at https://www.facebook.com/terms?ref=pf.
[775] Perez/Whittaker, "Facebook sues two companies engaged in data scraping operations", TechCrunch, 1 October 2020, available at: https://techcrunch.com/2020/10/01/facebook-sues-two-companies-engaged-in-data-scraping-operations/?guccounter=1.
[776] Sections 8.2(2) and (13) of the LinkedIn User Agreement, 1 February 2022, available at: https://www.linkedin.com/legal/user-agreement.
[777] US Supreme Court, order of 14 June 2021, see: https://www.supremecourt.gov/orders/courtorders/061421zor_6j36.pdf.
[778] US Court of Appeals for the 9th Circuit, opinion of 18 April 2022 in case no. 17-16783 , *HiQ Labs, Inc. v. LinkedIn, Corp.*, available at: https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2022-04-18.html.

that hiQ Labs had breached LinkedIn's terms and conditions both, through its own scraping of LinkedIn's site and using scraped data, on the one side, and through creating false identities on LinkedIn's platform.[779] In December 2022, LinkedIn and HiQ Labs reached a settlement agreement according to which HiQ Labs not only has agreed to pay half a million US Dollars as damages, but more importantly is also s permanently banned from scraping LinkedIn's platform as well as from developing, using, selling, or distributing any software or code (i.e. crawling tool) for data collection from LinkedIn platforms.[780]

In the EU, the use of a crawling tool for scraping content available on websites and especially on social media platforms could also constitute a breach of contract. The legal evaluation of private law contracts falls into the competence of national Member State law. According to Art. 5 TEU, the EU may adopt legislation only and insofar as the Member States have conferred appropriate competences upon it (*principle of conferred competences*). Although the Treaties do sometimes use the notion of 'private law', none of the rules conferring legislative competence upon the Union makes resort to this notion.[781] Because contract law is predominantly governed by national Member State law, only two key aspects can be pointed out for the lawful use of a crawling tool searching for specific content on a website or a social media platform:

The first question in contract law usually is whether a contract has been formed. Under German contract law for example, the mere visit of a website alone does not constitute a contract between the visitor and the website operator,[782] whereas the registration at a website or a social media platform forms a contract.[783]

If a contract is concluded according to national Member State law, *the second question* in contract law is whether the terms and conditions have become a valid part of the contract. Under German contract law, terms and conditions of a website become part of the contract for using its services when properly incorporated in the registration process. Therefore, the use of a crawling tool is in principle a breach of contract under German law, when the term and conditions prohibit crawling tools.[784] Only if the contractual

[779] US District Court for the Northern Distrct of California, decision of 4 November 2022 in case no. 17-cv-03301-EMC, *HiQ Labs, Inc. v. LinkedIn, Corp.*, available at: https://storage.courtlistener.com/recap/gov.uscourts.cand.312704/gov.uscourts.cand.312704.404.0.pdf; „Court Finds hiQ Breached LinkedIn's Terms Prohibiting Scraping, but in Mixed Ruling, Declines to Grant Summary Judgment to Either Party as to Certain Key Issues", The National Law Review, 11 November 2022, available at: https://www.natlawreview.com/article/court-finds-hiq-breached-linkedin-s-terms-prohibiting-scraping-mixed-ruling-declines.

[780] „hiQ and LinkedIn Reach Proposed Settlement in Landmark Scraping Case", The National Law Review, 8 December 2022, available at: https://www.natlawreview.com/article/hiq-and-linkedin-reach-proposed-settlement-landmark-scraping-case.

[781] Private law as such is not listed either among the *exclusive* (Art. 3 TFEU), or among the *supportive* (Art. 6 TFEU) competences of the EU. Therefore, private law belongs to the area of *shared* competences (Art. 4(2) TFEU) which address in particular the areas of: (a) internal market; (f) consumer protection; and (j) area of freedom, security and justice. Because the list of *shared* competences in Art. 4(2) TFEU is non-exhaustive, the EU has explicit competence in specifically designated areas of intellectual property law (Art. 118 TFEU), company law (Art. 50 TFEU) and labour law (Art. 153 TFEU). For an in-depth analysis of the EU competences in private law see: European Parliamentary Research Service (EPRS), "EU competence in private law", January 2015, written by Rafał Mańko and available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/545711/EPRS_IDA(2015)545711_REV1_EN.pdf.

[782] BGH (Federal Supreme Court), decision of 22 June 2011 in case no. I ZR 159/10, CR 2011, p. 757.

[783] Gausling, CR 2021, p. 609 (p. 611 at para. 10).

[784] Gausling, CR 2021, p. 609 (p. 611 at para. 11).

clause prohibiting the use of crawling tools was to violate a fundamental principle underlying statutory law, then the prohibiting clause could be considered invalid.[785]

In short: The legal evaluation of clauses prohibiting the use of crawling tools for accessing a website or a social media platform is complex and varies across national law in Member States and beyond. Especially since the crawling tool for the GRACE system is intended to search the internet globally, it seems recommendable to restrict their searches to known websites and social media platforms and conclude contractual agreements for accessing their content.

10.8. Future Legal Basis in Draft Regulation Against Online CSA

Most interesting in the context of the GRACE project, the investigatory powers of the Coordinating Authorities include the power to monitor compliance with the Draft Regulation Against Online CSA by conducting searches on publicly accessible material to detect known or new CSA material, Art. 31 Draft Regulation Against Online CSA. Therefore, Art. 31 Draft Regulation Against Online CSA provides a legal basis for Coordinating Authorities to carry out searches on publicly accessible material on hosting services in order to verify a provider's compliance in their jurisdiction. These searches are envisioned as automated using the indicators contained in the databases of indicators for known and unknown CSA material.[786]

[785] Gausling, CR 2021, p. 609 (p. 611 at paras. 12 et seq. and 15 et seq.).
[786] Art. 44(1)(a) and (b) Draft Regulation Against Online CSA.

11. Draft Cyber Resilience Act

In September 2022, the European Commission proposed a Regulation on cybersecurity requirements for products with digital elements which has become known as proposal for a Cyber Resilience Act (Draft CRA).[787] The core aim of the Draft CRA is to create cyber resilience and enhance cybersecurity for the entire IT supply chain[788] by setting standards for the design and development of all its components in an effort to reduce their vulnerabilities and improve their security throughout a product's life cycle.[789]

The Draft CRA would be fully applicable 24 months after its entry into force and, deviating from this, the reporting obligation of manufacturers comes into effect already after 12 months.[790] Bodies of the governance of the Member States would have to be in place before then. In particular, Member States would have appointed existing authorities or have to establish new authorities performing the tasks set out in this legislation.[791]

11.1. Scope

The Draft CRA regulates the "placing on the market of *products with digital elements*", pursuant to Art. 1(1)(a) Draft CRA. In Art. 3(1) Draft CRA, a *product with digital elements* is defined as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately". The GRACE system as a whole as well as each GRACE tools and the GRACE platform fall squarely under this definition of a *product with digital elements*. According to Art. Art. 1(1)(b) Draft CRA, the Draft CRA lays also down essential requirements not only for the production of *products with digital elements,* but also for their design and development.

Work Package WP10 is dedicated to analyse the market, define the most appropriate business models, and prepare an exploitation and long-term sustainability plan for the results of the project. Task T10.2 as well as Deliverables D10.3 and D10.4 are dedicated to elaborate an exploitation plan and business models for the post-project exploitation of the GRACE tools and platform in order bring the GRACE product and services to market via Alpha and Beta phases.[792] Hence, it cannot be excluded that the GRACE system or some of its parts could be placed on the EU market after a potential roll-out in the future. Against this background, the Draft CRA appears applicable to the design and development of the envisioned ATLANTIS system. This all the more so since the scope of the Draft CRA comprises any *products with digital elements* whose intended or

[787] Proposal for Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM (2022) 454 final, 15 September 2022, 2022/0272(COD); available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454.
[788] Explanatory Memorandum of the Draft CRA, p. 2.
[789] Rec. (2) Draft CRA; Explanatory Memorandum of the Draft CRA, p. 1.
[790] Art. 57(2) Draft CRA.
[791] Proposal for Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM (2022) 454, (55), p.28.
[792] GRACE Proposal Nr. 883341, p. 35 and 36.

reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network Art. 2(1) Draft CRA.

11.2. Cybersecurity Obligations

The Draft CRA contains an extensive catalogue of new cybersecurity obligations for each *economic operator* depending on their role and responsibility within the supply chain. According to Art. 3(17) Draft CRA, the term *economic operator* includes the *manufacturer*,[793] the *authorised representative*,[794] the *importer*,[795] and the *distributor*.[796] The lion share of cybersecurity obligations burdens the *manufacturer* in order to motivate them to incorporate sufficient cybersecurity already in the conceptualisation of a product.[797]

Manufacturers of *products with digital elements* must ensure that appropriate security measures are designed and implemented in accordance with the essential security requirements of the Draft CRA.[798] In order to comply with this obligation, *manufacturers* should assess the cybersecurity risks associated with a *product with digital elements* and take into account the result of this assessment in the planning, design, development, production, delivery and maintenance phases of the product to minimise cybersecurity vulnerabilities, prevent security incidents and mitigate the impact of such incidents with regard to the safety of users. This *cybersecurity risk assessment* should be part of the technical documentation for *products with digital elements* offered.[799] The list of essential security requirements includes a level of cybersecurity according to the CRA, a sales ban of products with known vulnerabilities, security by default configuration, protection against unauthorised access, limitation of attack surfaces and minimisation of the impact of incidents. Furthermore, the *products with digital elements* have to guarantee the confidentiality of the data, e.g. by encrypting data, protecting data integrity and only processing data that is strictly necessary for the product to function.[800]

In addition, *manufacturers* must monitor and fix vulnerabilities throughout the lifecycle for a maximum of 5 years, also through automatic and free updates.[801] The *manufacturers* are obliged to identify the weak points in their product through regular tests and to rectify them immediately.[802] The Draft CRA obliges *manufacturers* to report exploited vulnerabilities and incidents.[803] Possible exploited security vulnerability or incidents that could affect the security of *products with digital elements* have to be reported to *The European Union Agency for Cybersecurity* (ENISA) immediately, but no later than within 24 hours.

In addition to the obligation to report any kind of weak points of the product, *manufacturers* are obliged to label each product (CE marking) with digital components in such a way that consumers and users can identify

[793] As defined in Art. 3(18) Draft CRA.
[794] As defined in Art. 3(19) Draft CRA.
[795] As defined in Art. 3(20) Draft CRA.
[796] As defined in Art. 3(21) Draft CRA.
[797] Rec. (2) sentence 1 Draft CRA.
[798] Annex I of the Draft CRA on Essential Cybersecurity Requirements.
[799] Art. 10(3) Draft CRA.
[800] Annex I Section 1. No. (3) of the Draft CRA.
[801] Art. 10(12) Draft CRA in conjunction with Annex 1 of the Draft CRA on Essential Cybersecurity Requirements.
[802] Section 2. No. (1) – (8) of Annex II Draft CRA.
[803] Art. 11(1) and (2) Draft CRA.

and contact the *manufacturer*.[804] Member States shall build upon existing mechanisms to ensure correct application of the regime governing the CE marking and shall take appropriate action in the event of improper use of that marking.[805] The obligation applies also to *importers* and *distributors* of *products with digital elements*. They are also obliged to verify that the *manufacturer* has carried out the *conformity assessment procedure* and prepared the technical documentation.[806]

11.3. Conformity Assessment Procedure

The mandatory *conformity assessment procedure* for *products with digital elements* is regulated in Art. 24 Draft CRA and becomes increasingly stricter, the higher their level of cybersecurity risk is. The Draft CRA distinguishes between four different and increasing cybersecurity risk levels with matching *conformity assessment procedures*:

(1) *Products with digital elements* pose the lowest level of cybersecurity risks and their *cybersecurity assessment procedure* is regulated in Art. 24(1) Draft CRA.

(2) *Critical products with digital elements*[807] of class I as set out in Annex III of the Draft CRA for which the *cybersecurity assessment procedure* is regulated in Art. 24(2) Draft CRA.

(3) *Critical products with digital elements* of class II as set out in Annex III of the Draft CRA for which the *cybersecurity assessment procedure* is regulated in Art. 24(3) Draft CRA.

(4) *Highly critical products with digital elements*[808] pose the highest level of cybersecurity risks and their *cybersecurity assessment procedure* requires the *manufacturer* to obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to the Cybersecurity Act[809] to demonstrate conformity.

The envisioned GRACE system consists of many GRACE tools and the GRACE platform. As a whole, the GRACE system could be viewed as a Industrial Automation & Control Systems (IACS) in No. 22 of Class I as set out in Annex III of the Draft CRA.

---

[804] Art. 22 (*Rules and conditions for affixing the CE marking*), Annex II (Information and Instructions to the User) of Proposal for Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM (2022) 454, (55).

[805] Art. 22, 5. /Article 29 (*Requirements relating to notified bodies*) of Proposal for Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM (2022) 454, (55).

[806] Art. 13 Draft CRA.

[807] Defined in Art. 3(3) in conjunction with Art. 6(2) Draft CRA and Annex III of the Draft CRA.

[808] Defined in Art. 3(4) in conjunction with Art. 6(5) Draft CRA in delegated acts by the European Commission pursuant to Art. 50 Draft CRA.

[809] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Official Journal of the EU, 7 June 2019, L151, p. 51.

in addition to the potential future provider of the GRACE system qualifying as "managed service provider" also as *essential entity* under No. 9 in Annex I to the NIS2 Directive. Therefore, it would seem that the GRACE system would be evaluated in the *cybersecurity assessment procedure* for the third highest cybersecurity level as established in Art. 24(3) for *critical products with digital elements*, unless the European Commission were to specify categories in a delegated act pursuant to Art. 6(5) Draft CRA according to which the GRACE system would have to be considered as a *highly critical product with digital elements*.

It is very important to note, however, that Art. 8 Draft CRA regulates the coordination of the compliance procedures required under the Draft CRA and under the Draft AI Act for products regulated by the Draft CRA which are also classified as *high-risk AI systems* under the Draft AI Act. The GRACE system constitutes a *critical product with digital elements* listed in Annex III to the Draft CRA and classifies as *high-risk AI system* according to Art. 6 Draft AI Act (section 5.2.2 above). Because this dual qualification, the future GRACE system will have to undergo the conformity assessment procedure pursuant Art. 19(1) Draft AI Act in conjunction with Art. 43 Draft AI Act and the GRACE system will also have to undergo the conformity assessment procedure required in Art. 24(3) Draft CRA in so far as the essential requirements of the Draft CRA are concerned, Art. 8(2) Draft CRA.

12. Considerations Towards Future Standards

This chapter addresses the final part of Task T9.2 and, based on the results of the analysis, contemplates and attempts to formulate recommendations in support of defining potential future standard protocols, procedures and data formats for international and cross-border approved exchange of information and court proof-evidence among LEAs.

The platform and tools developed in the course of the GRACE project (the GRACE system) are envisioned for analysing, categorising and managing the data contained in CSEM reports. From a purely investigative point of view, among the first steps of an investigation is the verification of facts followed by an update of the evidence which typically includes a search for additional evidence regarding the investigated suspect(s). In this respect, it would be convenient for LEAs to be able to automatically check the data-set of a CSEM report with accessible databases within the law enforcement ecosystem, on the one hand, and with Open Source Intelligence (OSINT) in the EU for additional information concerning suspects.

In this context, there are only few drafts of EU-legislation in place establishing some standards for narrowly defined areas including on particular types of data and on particular communication channels. However, the legal approaches to define standards tend to remain at a highly abstract level and only rarely refer to specific technological solutions. While this provides necessary wriggle-room for technological innovations, the range of suitable technological solutions would potentially benefit from some common standard protocols, procedures and data formats. The development of the GRACE system has involved several key decisions on the architecture and design which might serve as helpful recommendations in support of defining potential future standard protocols, procedures and data formats for international and cross-border approved exchange of information and court proof-evidence among LEAs.

The legal approaches for regulating future standards in these areas are briefly described as they appear in current draft legislation at EU level (section 12.1. below). In view of legal approaches either focussing on content or devolving the power of setting specific technical standards in certain areas to key institutions, it is then highlighted which of the technical solutions selected for the GRACE system might be considered as recommendation in support of defining standard protocols, procedures and data formats in the future (section 12.2. below).

12.1. Legal Approaches to Standards

The legal approaches for regulating future standards international, cross-border approved exchange of information or court-proof evidence by LEAs appear in current draft legislation at EU level. In addition, there are national standards as detailed for the selected Member States in the five Country Reports below.[810]

12.1.1. Cross-Border Exchange of Information

The Draft Prüm II Regulation (described in section 2.3.3 above) envisages to facilitate automated data

[810] The five Country Reports are on: Slovenia (chapter 13.), Cyprus (chapter 14.), Portugal (chapter 15.), Germany (chapter 16.) and Lithuania (chapter 17.).

exchange between LEAs in different Member States and with Europol as the EU criminal information hub.[811] By introducing facial images, police records and driving licence data as additional categories data eligible to automated comparison, the Draft Prüm II Regulation proposes to establish a new infrastructure for standardised procedures identifying a match of core data. The technological architecture for such queries, consisting of the Prüm II router[812] for comparisons of biometric data and European Police Records Index System (EPRIS)[813] for comparisons of police records, is envisaged the use of the **Universal Message Format (UMF) standard** in the development of each of these two central routers, Art. 34(1) Draft Prüm II Regulation. In addition, any automated exchange of data in accordance with the Draft Prüm II Regulation is expected to use the UMF standard.[814] As a consequence, the UMF standard has the potential to become the nascent standard for exchanging information about the content of law enforcement databases and for that reason merits a closer look.

The UMF standard was introduced in two Regulations in 2019 aiming to harmonise the exchange of information in a particular area of cross-border police and judicial cooperation: Regulation (EU) 2019/818[815] together with Regulation (EU) 2019/817[816] established a framework to ensure interoperability between the EU information systems in the field of borders, visa, police and judicial cooperation, asylum and migration. These two Regulations establish in their respective Art. 38(1) the universal message format (UMF) to serve as a standard for structured cross-border information exchange between information systems, authorities or organisations in the field of Justice and Home Affairs. Art. 38(3) Regulation (EU) 2019/818 confers the power onto the European Commission to adopt an implementing act to lay down and develop the UMF standard. In February 2023,[817] the European Commission laid down the specific UMF standard requirements[818] which shall be used to describe information exchanged between information systems in the field of Justice and Home Affairs.[819] The UMF standard may be used for the exchange of information between information systems, authorities or organisations,[820] but is not mandatory for the description of data elements stored in an information system or database.[821] The UMF standard shall be used for the development of the European

[811] Proposal for a Regulation of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM/2021/782 final, 8 December 2021, Explanatory Memorandum, p. 2. See also sections 7.2.2.5 and 9.5 above.
[812] Art. 35 Draft Prüm II Regulation.
[813] Art. 42 Draft Prüm II Regulation.
[814] Art. 34(2) and Rec.(19) Draft Prüm II Regulation.
[815] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, 22 May 2019, Official Journal of the EU L 135, p. 85.
[816] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, 22 May 2019, Official Journal of the EU L 135, p. 27.
[817] Commission Implementing Decision (EU) 2023/221 of 1 February 2023, Official Journal of the EU L 30, p. 26.
[818] Art. 2(1) in conjunction with Annex I of Commission Implementing Decision (EU) 2023/221.
[819] Art. 3(2) of Commission Implementing Decision (EU) 2023/221.
[820] Art. 3(1) of Commission Implementing Decision (EU) 2023/221.
[821] Art. 3(3) of Commission Implementing Decision (EU) 2023/221.

search portal (ESP)[822] as well as for the information exchanged with the common identity repository (CIR) and the multiple-identity detector (MID) as provided for in Regulation (EU) 2019/818.[823] Furthermore, Annex II of Regulation (EU) 2019/818 provides specific elements for labelling data fields which are derived from the UMF standard and shall be used in the development of the European Asylum Dactyloscopy Database (Eurodac), the European Criminal Records Information System for third-country nationals (ECRIS-TCN) as well as of the ESP, the CIR and the MID.[824]

The European Commission also suggested in Art. 48 Draft Prüm II Regulation to establish the platform **Secure Information Exchange Network Application (SIENA)**[825] as the default system for any exchange between MS LEAs and with Europol outside the scope of the Draft Prüm II Regulation. However, because Art. 48 Draft Prüm II Regulation appears deleted in the General Approach of the Council,[826] the role of SIENA in the context of information exchange in the scope of a future Prüm II Regulation remains to be seen. The role of SIENA is central in the Draft Directive on Information Exchange between MS LEAs[827] which proposes to ensure that not only every national Single Point of Contact, but also any MS LEA involved in the exchange of information under this Directive, are directly connected to SIENA and conduct the information exchange through SIENA, Art. 13 Draft Directive on Information Exchange between MS LEAs. The General Approach of the Council suggests to allow in an additional Art. 13(1a) four significant exceptions to the use of SIENA in case the exchange of information: (a) was initiated by Interpol, (b) involves a third country or international organisation not connected to SIENA, (c) can be faster with another communication channel for urgent requests, or (d) where unexpected technical or operational incidents suggest the use of another channel for the information exchange between MS.[828] Therefore, the ultimate role of SIENA also remains to be seen in the context of information exchange in the scope of a future Directive on Information Exchange between MS LEAs.

[822] Art. 4 of Commission Implementing Decision (EU) 2023/221.
[823] Art. 5 of Commission Implementing Decision (EU) 2023/221.
[824] Art. 2(3) in conjunction with Annex II of Commission Implementing Decision (EU) 2023/221.
[825] Europol, „Secure Information Exchange Network Application (SIENA)“: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena.
[826] Council of the EU, „Council adopts two general approaches and a recommendation to improve operational police cooperation and information exchange“, Press Release, 10 June 2022, linking to the General Approach of the Council on the Draft Prüm II Regulation, No. 9544/22, 31 May 2022, available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/10/council-adopts-recommendation-two-negotiating-mandates-improve-operational-police-cooperation-information-exchange/.
[827] Proposal for a Regulation of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM/2021/782 final, 8 December 2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:782:FIN.
[828] Council of the EU, „Council adopts two general approaches and a recommendation to improve operational police cooperation and information exchange“, Press Release, 10 June 2022, linking to the General Approach of the Council on the Draft Directive on Information exchange between MS LEAs, No. 9544/22, 31 May 2022, available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/10/council-adopts-recommendation-two-negotiating-mandates-improve-operational-police-cooperation-information-exchange/.

12.1.2. Cross-Border Exchange of Court-Proof Evidence

Standardising the channels for cooperation, the eEvidence Regulation[829] introduces five clear and user-friendly forms in its annexes: the "European Production Order Certificate (EPOC) for the production of electronic evidence" in Annex I; the "European Preservation Order Certificate (EPOC-PR) for the preservation of electronic evidence" in Annex II, the "Information on the impossibility to execute the EPOC / EPOC-PR" in Annex III, the "Confirmation of Issuance of request for production following a European Preservation Order" in Annex IV and the "Extension of the preservation of electronic evidence" in Annex V. While these five forms concern the content of what is communicated to whom, Art. 18d eEvidence Regulation confers implementing powers onto the European Commission for establishing the decentralised IT system by setting out: (i) the technical specifications defining the methods of communication by electronic means for the purposes of the decentralised IT system; (ii) the technical specifications for communication protocols; (iii) the relevant technical measures ensuring minimum information security standards and a high level of cybersecurity for the processing and communication of information within the decentralised IT system, and (iv) the technical requirements for the services provided by the decentralised IT system to meet their minimum availability objectives.

12.2. Practical Approach to Standards for GRACE System

Developing the most appropriate architecture and design for the GRACE system involves several key decisions about selecting state-of-the-art protocols, procedures and data formats for integration and use in the GRACE system. From a practical perspective, these specific protocols, procedures and data formats for the GRACE system might serve as recommendations in support of defining potential future standards for international and cross-border approved exchange of information and court proof-evidence among LEAs.

The **general architecture** of the GRACE system is refined in the Deliverables on "Technical and Architecture Specification" the currently available iteration of which is Deliverable D2.12 "Technical and Architecture Specification v3" which will be finalised in D2.13. Relying on best practices to adopt modern design approaches and to address common design challenges such as defining cross-cutting concerns, the design of the GRACE system's microservices architecture consists of a set of loosely-coupled services developed as standalone components capable of using standard technology-agnostic interfaces to interact with each other.[830]

[829] Council of the EU, Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, final compromise text, 5448/23, 20 January 2023, available at: https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf.

[830] Section 2.1.1 of Deliverable D2.12.

The **data ingested** in the GRACE system stems from three different sources: (i) referrals by NCMEC/NCCEC via a dedicated REST API;[831] (ii) digital media uploaded by LEAs on demand;[832] and (iii) targeted web crawler collecting open source intelligence (targeted OSINT).[833] The architecture and specifications of the targeted OSINT crawler is detailed in classified Annex of Deliverable 3.2 "Data Acquisition Modul v2".

Hashing: The data processing by the GRACE system includes hashing on initial data ingestion. In NCMEC referrals, the exchange file formats, hashes of uploaded files (CSAM), are (usually) in the XML/JSON. Normally the applied hashing functions during the pre-processing are **traditional hashing** algorithms (MD5 or SHA1) allowing identification of byte-identical files only.[834] In comparison, **robust hashing** algorithms offer a certain level of tolerance which allows to search for files which are binary different, but may still contain visually similar content (encoded in different file formats, possibly resized or cropped content etc.). Robust hashing algorithms are used both for digital still images and digital video-audio recording in order to enable deduplication and analysis purposes in the following data processing and analysis stages.[835] Concerning still images, not only the *de facto* industry standard PhotoDNA by Microsoft but also four different open source algorithms have been considered for the GRACE system: (1) phash; (2) dhash, (3) whash and (4) PDQ.[836] Concerning videos, two *de facto* industry standards (PhotoDNA for Video by Microsoft and F1 by Friend MTS, both sub-licensed to selected institutions by NCMEC via Project VIC) and the open source algorithm TMK+PDQF by Facebook have been considered for the GRACE system as well as a range of solutions suggested by the scientific community.[837] While the use of PhotoDNA involved challenging licensing issues which could not be resolved for the GRACE project, robust hashing functionalities for still images and videos are provided via the alternative algorithms.[838] Regarding still pictures, the robust hashing service currently uses the perception python library implementing as a minimum the three most widely adopted hashing algorithms (PHash, DHash and PDQ), whereas the development of robust hashing for videos will be considered at a later stage[839] because each of the alternative algorithms presents robust behaviour only to some type of (video) transformations while being sensitive to some others.[840]

The GRACE system's microservice providing **Chain of Custody** (CoC) tracks the accesses to and the operations with the stored resources in the GRACE system in order to prove that the originality and integrity of these

[831] Section 3.2.1.1 of Deliverable D2.12.
[832] Section 3.2.1.2 of Deliverable D2.12 for forensic data and section 3.2.1.4 of Deliverable D2.12 for structured data.
[833] Section 3.2.1.3 of Deliverable D2.12.
[834] Section 3.1 of Deliverable D3.11.
[835] Robust hashing provides a capability to match media files regardless their source; however, the traditional hashing ensures exact binary matching of (media) files within the GRACE environment.. For a detailed description of the pre-processing process see section 5.1.2 of Deliverable D2.2.
[836] Section 3.3. of Deliverable D3.11.
[837] Section 3.3. of Deliverable D3.11.
[838] Although implementing de facto industry standards in the GRACE system was a high priority, not even a temporary development licensing agreement for NICC (= main developer of these technologies within GRACE) had been reached at month M23 of the GRACE project (section 3.3. of Deliverable D3.11) and the third iteration of the "content management and digital evidence tamper detection module" in Deliverable D3.12 prensents in section 3.6. the reasons for providing robust hashing functionalities for pictures and videos in the GRACE system via alternative technologies.
[839] Section 3.6 of Deliverable D3.12.
[840] Section 3.3 of Deliverable D3.11.

resources have been maintained since the acquisition time.[841] In order to detect any form of tampering or manipulation either by a person or by components operating within the GRACE system, time stampers are logging in compliance with the RFC3161 time-stamp protocol.[842] To enable a description of all the details of the logging process activity[843] the data are organised into a JSON string when pushed to the CoC logging service[844] which will then interact with the WP7 Orchestrator Framework and the WP3 Orchestrator.[845]

Watermarking: For the GRACE system, watermarking serves to enable a process for verifying the authenticity and integrity of media content exported by the GRACE system to third parties and to preserve the media content's admissibility in court. For that purpose, any digital GRACE artefact (e.g., a picture, audio or video file) will be watermarked and newly hashed before being exported, while a copy of the watermarked GRACE will be stored on the GRACE platform and not only the watermark URI, but in addition, also the hash of the watermarked GRACE artefact will be stored by the GRACE watermarking module.[846] Such watermarking services have been developed for the GRACE system and comply with the REST + broker communication protocol to allow for their integration into pipeline data flows,[847] but it is currently still explored whether and which data would have to be watermarked or whether LEAs might prefer alternative ways (non-watermarked) of exporting results (which and how).

Report Exporter: From a practical perspective, the GRACE system has to be interoperable with the Europol IT-architecture in general[848] and the tool responsible for exporting and disseminating reports from the GRACE system to MS LEAs has to be compatible with the Europol case management in particular. Therefore, this exporting the reports generated by the GRACE system (report exporter) is able to use the SIENA channel and assigns to each report a SIENA number.[849] This capability to use the SIENA channel lays the ground to fulfil any legal requirement to use SIENA in the future Prüm II Regulation or in the future Directive on Information Exchange between MS LEAs, at the same time.

[841] Section 3.8 of Deliverable D2.12.
[842] Section 6.2 of Deliverable D7.4 for the focus on Trusted Third Party (TTP, "stamper") approach. The selected time-stamp protocol is yet to be confirmed in Deliverable D7.5.
[843] Apart from time, section 6.6 of Deliverable D7.4 outlines: (1) the user, (2) the activity, (3) the affected input item and output items, and (4) additional input parameters provided to the transformation.
[844] Section 6.6 of Deliverable D7.4.
[845] Section 6.5 of Deliverable D7.4.
[846] Section 4.1 of Deliverable D3.11.
[847] Section 4.5 of Deliverable 3.12.
[848] Section 2. of Deliverable D2.12.
[849] Section 3.4 of Deliverable D2.12.

13. Country Report on Slovenia

This chapter aims to outline the legal framework regulating the fight of law enforcement agencies (LEAs) against child sexual exploitation (CSE) and child sexual exploitation materials (CSEM) in Slovenia.

13.1. Victim's Rights[850]

A person will be considered as victim of a crime if he/she has been harmed (that is physically injured, property has been damaged or confiscated etc.) for an act considered a crime under national law. In addition, a victim of a crime is a person who has suffered direct damage as a result of the crime as a provable consequence of that crime. This means that a victim has suffered physical or mental consequences as a result of the offense or that her/his property has been damaged, destroyed or confiscated because of a criminal offense under national criminal law.

For a victim of crime, the law guarantees certain individual rights before, during and after a court proceeding (trial).

As an illustration, below is an extensive list of the victims' rights in Slovenian legal framework:

- to particularly careful and considerate treatment for reasons of vulnerability, such as age, health, disability or other similar circumstances;[851]
- to use its own language or a language he or she understands;[852]
- to be accompanied by a trusted person chosen by him- or herself when making initial contact with a competent authority;[853]
- to be represented in proceedings by an authorised representative, who may be a lawyer; if a person is a minor-victim of certain crime offences, the representative will be appointed by the court if he or she has not selected one for him- or herself beforehand;[854]
- to get free health, psychological and other care and to support offered by social services' centres and other organisations;[855]
- to be apprised of assistance options and of other legal measures;[856]
- to have any undesired contact with the perpetrator prevented, unless contact is indispensable to the successful performance of pre-criminal or criminal procedure;[857]

---

[850] A basis for this contribution was taken from the official website of Slovenian Government and Ministry of Justice, at: https://www.gov.si/teme/pravice-zrtev-kaznivih-dejanj/.
[851] Article 18a of the Criminal Procedure Act (CPA), Official Gazette of the Republic of Slovenia [OGRS], no. 176/2021 – Official Consolidated Text.
[852] Article 8 of the CPA.
[853] Article 65(4) of the CPA.
[854] Article 65 of the CPA.
[855] Article 65a(1)(1) of the CPA, Article 14a of the Social Assistance Act (SAA), OGRS, no. 28/2019.
[856] Article 65a(1)(2) of the CPA, Domestic Violence Prevention Act (DVPA), OGRS, no. 16.2008 and 68/2016.
[857] Article 65(5) of the CPA.

- to be notified of the release or escape of a suspect or the accused from detention or house detention for the purposes of securing his or hers personal safety;[858]
- to request information on the departure, release or escape of a prisoner;[859]
- to protective and other measures to ensure personal safety, such as:
  - recording a testimony if a witness is under 15 years of age;[860]
  - being questioned (before the police) by the same person or a person of the same gender;[861]
  - testify with the assistance of an expert and in specially adapted premises;[862]
  - having witnesses' personal data protected and testify by using technical resources such as a protective screen;[863]
  - testify via video link;[864]
  - exclusion of the public from the main hearing;[865]
- to have the rights when those are referred to minor-victim[866] also being respected by an expert who examines or interviews the minor-victim in order to draw up an expert opinion;[867]
- to receive confirmation or a copy of the record upon reporting a criminal offence[868];
- to receive information on the course of his or her case and on his or her role in pre-criminal or criminal procedure;[869]
- to be provided with the details of a contact person at the competent authority with whom he or she may communicate on his or her case;[870]
- to highlight facts, propose evidence, and view and copy the case file in criminal procedure;[871]
- to give his or her opinion on any intended dismissal of a criminal complaint regarding a criminal offence for which the law prescribes a prison sentence of more than eight years;[872]

[858] Article 65a(4) of the CPA.
[859] Article 30b of the Enforcement of Criminal Sanctions Act (ECSA), OGRS, no. 11/2018.

[860] Article 84(1) of the CPA.
[861] Article 148b of the CPA.
[862] Articles 240(5) and 240(6) of the CPA.
[863] Article 240a of the CPA.
[864] Article 244a(1) of the CPA.
[865] Article 295 of the CPA.
[866] Enshrined in the Articles 65(5) and 240(6) of the CPA.
[867] Articles 264 and 264a of the CPA.
[868] Article 147a of the CPA.
[869] Article 65a(3) of the CPA.
[870] Article 65a(1)(8) of the CPA.
[871] Article 59 of the CPA.
[872] Article 161(4) of the CPA.

- to take charge of prosecution if it is not commenced or is abandoned by the state prosecutor;[873]
- to file a motion to enforce a claim for indemnification;[874]
- to receive free legal aid under the Legal Aid Act;
- under the Crime Victim Compensation Act,[875] to be apprised of the method and conditions applying to exercise of the right to compensation for victims of intentional criminal offences involving violence;
- to the payment and reimbursement of costs incurred in criminal procedure;[876]
- to file an appeal against a judgment.[877]

Regardless of whether a victim files a criminal complaint, under the SAA and as the victim of a crime offence that has directly caused the victim to suffer damage of any kind, such a victim is entitled to support for victims of crime. This includes specialist support and counselling provided by social services centres. This enables the victim to receive psychological, social and financial relief from the position into which the victim has been placed by the crime.

Meaningfully equal rights of victims can also be used, when a victim of a crime gets in contact with the police authorities in Slovenia.

Additionally, one of the main principles for the performing of the police duties is the principle of respect for human personality and dignity as well as other human rights and fundamental freedoms, enshrined in Article 13 of the Police Tasks and Powers Act (PTPA).[878] This provision emphasizes that police officers must treat victims and persons who need additional attention, help and care, such as children, minors, the elderly, disabled persons, pregnant women and victims of domestic violence, with special consideration. As already said, this undoubtedly applies to victims of violent crimes, which sexual abuse of children and sexual exploitation of children undoubtedly are.

13.1.1. The Right to Protective and Other Measures to Ensure Personal Security (Witness Protection)

In 2005, Slovenia introduced its very first Witness Protection Act (WPA),[879] which aims at regulating the protection of the victims. This act is based on CPA, which defines quite a few protective measures, while the WPA established principles for witness protection, created a unit and a committee for the protection of

[873] Articles 60 and 63(2) of the CPA.
[874] Articles 100–111 of the CPA.
[875] CVCA, OGRS, no. 101/2005 and 114/2006, available at: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4264#. See for more in the subchapter on Compensation for Victims.
[876] Articles 92, 96(4) and 97 of the CPA.
[877] Article 367(4) of the CPA.
[878] OGRS, no. 15/2013, 23/2015, 10/2017, 46/2019 – Decision CC, 47/2019 and 153/2021 – Decision CC.
[879] Summary made from Witness Protection Act (orig. Zakon o zaščiti prič - ZZPrič), OGRS, no. 81/2006, 110/2007 and 30/2018, available at: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4265#

endangered individuals. It outlines conditions and procedures for inclusion in the protection program, including the termination of the program, data protection, financing, and oversight.

Not all witnesses are endangered, but still there are individuals (witnesses and victims), who are at risk due to their involvement in criminal cases. The WPA facilitates cooperation between Slovenian authorities and those of other countries in safeguarding these individuals. Inclusion in the protection program requires voluntary written consent, and authorities must inform the witness about the potential impact on their life and the rights that may be restricted.

The unit for the protection of endangered individuals will be responsible for implementing protective measures and proposing actions within the program. The WPA allows for concealing the true identity of protected witnesses and unit employees. The committee for the protection of endangered individuals, consists of members from a supreme court and representatives from relevant ministries that are overseeing the process.

The committee must decide promptly whether to initiate the inclusion process in the protection program based on a proposal from the public prosecutor's office. The unit evaluates the feasibility of the program and collects personal information about the endangered witness. Not all individuals may qualify for inclusion and may undergo a comprehensive medical examination, including psychological testing.

Protected individuals must follow program instructions and keep information about their location, work, and new identity confidential. They are restricted from visiting previous locations and must promptly inform the unit of any changes.

The unit provides psychological, financial, and legal assistance to protected individuals in addition to implementing program measures. Urgent protective measures as part of the program measures include counselling by the unit, technical and physical protection of persons or residences, temporary relocation of persons, as well as issuance of modified documents and change of identity.

The Witness Protection Act is a systemic law that enables the protection of important witnesses in serious criminal offenses if their life or the body or the life or body of another endangered person is seriously endangered and protective measures are necessary to avert danger.

13.1.2. Compensation for Victims

The right to be acquainted with the manner and conditions of exercising the right to compensation to victims of violent intentional criminal offenses is regulated in the Crime Victim Compensation Act (CVCA).[880] The condition for claiming compensation as victim or as relative of a victim is that the individual is a citizen of the Republic of Slovenia or another EU Member State.

The victim, a victim of violent intent, in particular a crime against life and limb or sexual integrity, may claim compensation from the state under the CVCA. Under certain conditions, the relative of a victim can also claim compensation, if the victim has lost his/her life due to the crime.

[880] Summary made from Crime Victim Compensation Act.

In cases where the perpetrator of the violent intent is unknown or cannot be prosecuted because, for example, the perpetrator is deceased, the victim or a relative does not have to claim compensation from the perpetrator first. Victim is also entitled to such a special position if, at the time of the commission of the offense, was under the age of 18 or a child, a victim of domestic violence, a disabled person or a foreigner, i.e. a citizen of another EU Member State. The deadline for filing a claim for damages in these cases is six months from the commission of the offense.

In the remaining cases, compensation for the damage from the offender must first be claimed.

If enforcement is not successful or not possible at all, then compensation can be claimed from the state under the CVCA. In these cases, the deadline for claiming compensation is three months from the receipt of information on the failure or impossibility of enforcement, for example, from the receipt of the decision to suspend enforcement, from responses to inquiries about the perpetrator's property and the like.

The victim or a relative can file a claim for compensation on the prescribed form with the Ministry of Justice.[881]

13.2. Criminal Procedure

A victim is a person who has been harmed by a criminal act[882] and as a consequence, when talking about a natural person, it can result in physical, mental, sexual, emotional, or economic harm. According to the CPA, if a person dies as a result of a criminal act, their spouse, a person in a conjugal relationship, blood relatives in the same line, their adopted child or adoptive parent, their brothers and sisters and persons whom they supported or were obliged to support are also considered victims. Therefore, the violated rights of the injured party can be personal or any property right. This means that in criminal proceedings the victim can be both a natural person and a legal entity.

Victims have the option to report a criminal act or file a complaint with either the state prosecutor or the police.

The police must accept the complaint and forward it to the appropriate state prosecutor.

Reporting a complaint to the police can be done in person at any police station or department, via phone, in writing or via online tools. After receiving a complaint, the police officers assess whether there is reasonable suspicion that a crime has occurred and take necessary measures to identify and apprehend the perpetrator, secure evidence and crime scene traces, and collect relevant information for the successful execution of the criminal procedure.

[881] More detailed information are available at:

http://mp.arhiv-spletisc.gov.si/si/delovna_podrocja/direktorat_za_kaznovalno_pravo_in_clovekove_pravice/sektor_za_popravo_krivic_in_podporo_zrtvam_kaznivih_dejanj/odskodnine_zrtvam_kaznivih_dejanj/index.html

[882] Kovač, J. (2022). Pravni položaj oškodovanca v Zakonu o kazenskem postopku, Pravna praksa, no. 31-32/2022, p. 16 – 18.

The police collect information and evidence based on the victim's report, which is crucial for the subsequent criminal proceedings. Following the instructions of the state prosecutor, they prepare a criminal complaint with relevant evidence to support the procedure. This compilation is then sent to the state prosecutor, who ultimately decides whether to proceed and how.

The state prosecutor can dismiss the criminal complaint, request additional information, and propose a settlement with the victim's consent. The settlement involves the offender performing community service or taking actions to mitigate or eliminate the harmful consequences of the crime. If the settlement is fulfilled, the complaint is dismissed. Alternatively, the state prosecutor may directly submit an indictment to the courts or request further investigative actions conducted by an investigating judge. During the trial, the court reviews the gathered evidence and determines the guilt of the perpetrator. If found guilty, the court imposes an appropriate punishment.

On the other hand, the Criminal Code[883] governs the proceedings related to criminal offenses, while the CPA establishes the procedural rules aimed at ensuring the fair treatment of individuals, preventing wrongful convictions. A person accused of a criminal offense is presumed innocent until proven guilty through a final judgment. The primary objective of criminal proceedings is to determine the guilt of the offender and impose an appropriate sanction for the committed offense. In Slovenia, criminal proceedings consist of multiple stages.[884] It is essential to keep track of these stages as they shape the defendant's position and involve various procedural steps. The stages from the above summarized presentation of the criminal proceedings can be divided into four main stages:

(a) Pre-trial proceedings: Upon the report or filing of a criminal complaint, the police investigate the actual circumstances surrounding the offense. Alongside the evidence, the complaint is then forwarded to the state prosecutor, who has the authority to dismiss the complaint, request a court investigation, or directly file an indictment.[885]

(b) Judicial investigation: The investigative phase commences with the investigating judge, who examines the police materials and fulfils the state prosecution service's requests for further inquiry. The court investigates the details of the criminal offense and collects evidence for use in subsequent stages of the criminal proceedings.[886]

(c) Trials: The specific phase, whether held at the local or district court, depends on the severity of the prescribed sanction for a particular criminal offense.[887]

(d) Appealing stage: Within 30 days of receiving the written judgment issued by the local or district court, clients have the right to appeal. A higher court then reviews the appeal and makes a decision accordingly.[888]

[883] OGRS, no. 50/2012-OCT, 6/2016-correct., 54/2015, 38/2016, 27/2017, 23/2020, 91/2020, 95/2021, 186/2021 and 16/2023.
[884] See: https://www.dt-rs.si/criminal-proceedings
[885] See previous.
[886] See previous.
[887] See previous.
[888] See previous.

Directing the criminal investigation in the so-called pre-trial proceedings are in the domain of the competent state prosecutor. The police, police officers and crime detectives are obliged to follow the directions and instructions of the competent state prosecutor's office.[889]

In any case, it is of great importance to timely inform the competent state prosecutor's office about new circumstances of the crime or evidence, which means that the prosecutor will be able to properly direct the work of the police and later more adequately represent the indictment in court proceedings.

13.3. Data Protection

The right to data privacy and the protection of personal data in Slovenia is guaranteed by Article 38 of the Constitution of the Republic of Slovenia.[890] The protection of personal data is raised to the same position as the right of communication privacy and freedom of expression.[891]

The special feature of constitutional decrees is the requirement that the law determines the collection, processing, purpose, control and protection of the secrecy of personal data.

The Personal Data Protection Act (ZVOP-1) 2004, although amended several times, was until recently representing the Slovenian national legislation on personal data protection. The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data was transposed into this ZVOP-1 2004. Namely, Slovenia was the only EU country without the implementing act of GDPR until the newly passed Personal Data Protection Act (ZVOP-2) which came into effect on 26th of January 2023.[892]

[889] The relationship between the State Prosecutor and Police (and other competent bodies) are defined in the Decree on the cooperation of the state prosecutorial service, Police and other competent state bodies and institutions in detection and prosecution of perpetrators of criminal offences and operation of specialised and joint investigation teams, OGRS, no. 83/2010 and 28/2021.

[890] Article 38 of the Constitution stipulates the following:
Protection of Personal Data

(1) The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.

(2) The collection, processing, designated use, supervision, and protection of the confidentiality of personal data shall be provided by law.

(3) Everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data.

[891] https://www.dataguidance.com/notes/slovenia-data-protection-overview

[892] OGRS, no. 163/2022, available at: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7959

Due to the lack of the legislation, the Information Commissioner[893] was more or less without the relevant power to impose fines and consequently has not been able to impose any of the administrative fines since the adoption of the General Data Protection Regulation.[894]

The new law aims to bring the country's data protection framework in line with the GDPR. According to the provisions of the General Regulation, the national regulation can regulate certain substantive areas, such as the use of health, biometric and genetic data, certain procedural aspects (e.g. the procedure for imposing sanctions and legal remedies) and the relationship to other areas and rights (e.g. access to public information character, use of personal data for research, archival and statistical purposes).[895]

Finally, the ZVOP-2 regulates the implementation of human rights to personal data protection. It includes obligations, principles, entitlements, procedures and measures that ensure constitutional compliance, legality and justification of interventions in privacy, dignity, confidentiality of personal data, data self-determination or other fundamental rights of individuals in the processing of personal data and rules on the free flow of personal data for the implementation of the GDPR and other issues related to the processing and protection of personal data.

The Slovenian Information Commissioner explains that it regulates additional conditions for authorized persons for data protection, changes the regulation of video surveillance, assurance of traceability and some other areas. However, ZVOP-2 may not change the provisions of the GDPR, as the regulation must be directly applied. It should be taken into account that both the General Regulation and ZVOP-2 apply, so the provisions of ZVOP-2 must also be read in the light of the GDPR (ibid.).

The provisions of the ZVOP-2 do not apply to questions related to the protection and processing of personal data governed by the legislation of the personal data in criminal proceedings.

13.4. The Police and Victim Identification Function

Slovenia has one police organisation, which operates at three levels (national, regional and local).

Among other departments within the Police, the Criminal Police Directorate at national level, Criminal Police Divisions at regional level and Police stations at local level (among other tasks) are responsible to perform various tasks related to detection, investigation and prevention of criminal offences. Crimes against sexual exploitation and abuse of children are the domain of Criminal police at national and regional level.

Slovenia does not have a separate department or group solely responsible for identification of sexually abused children over the internet. Criminal investigators in the Juvenile Crime Section (national level) and Juvenile

[893] Information Commissioner is an autonomous and independent body, established on 31. December 2005, which supervises both the protection of personal data, as well as access to public information. https://www.ip-rs.si/en/about/competences/

[894] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR); it entered into force on 25 May 2016 and has been directly applicable since 25 May 2018.

[895] https://www.ip-rs.si/zakonodaja/zakon-o-varstvu-osebnih-podatkov/zvop-2

Crime Groups (regional level) carry out the identification of sexual abuse of children. Police stations usually do not perform investigations sexual crimes against children, unless in close cooperation with the regional units.

In the Child Sexual Abuse Material (CSAM) cases, criminal investigators from the Computer Investigation Centre (national level) and its sections at regional level (unofficially known as Cybercrime Investigation units) insure the contents of seized electronic devices and extracts information that might be relevant for the case and all the CSAM. The investigators of Juvenile Crime Section/Groups are those who substantially evaluate the secured material and perform identification of victims, and their safeguarding.

13.4.1. Processing of Personal Data by the Police

Beside the legislation provided in sections 13.1, 13.2 and 13.3 above, the specific law provides the legal basis for the Police to process personal data. This is the Police Tasks And Powers Act - PTPA[896], which in its chapter 5 regulates data collection and processing.

The general provision is Article 112 PTPA (data collection), which states the following:

> *(1) In the performance of police tasks, police officers shall collect and process personal and other data, including biometric data and data arising from confidential relationships or professional secrets. Police officers may process data during the identification procedure and in the detection and investigation of criminal offences. In the detection and investigation of criminal offences police officers may, if necessary and required given the circumstances of a concrete criminal offence, compare finger and palm prints, photographs with photographs of other persons and compare DNA profiles. These data may be processed in an automated manner.*
>
> *(2) Police officers shall acquire personal and other data directly from the person to whom they refer and from others who may have such information, or from personal data filing systems, official records, public registers or other data bases. The police must preserve the confidentiality of the source of a report or message.*
>
> *(3) The police may record and reconstruct those electronic communications in their information and telecommunication system that are intended for the performance of police tasks and are conducted within the police or with other state authorities or holders of public authority. In accordance with the law, the recordings or their reconstructions may be processed in order to verify the legality and professional competence of police procedures and measures in the performance of police tasks. The participants in the communication must be informed in advance that the communication will be recorded and of the purpose of recording.*
>
> *(4) During a pre-trial investigation concerning the criminal offences referred to in Articles 170 to 176 of the Criminal Code (KZ-1) that have been committed against a minor, for the purposes of seeking suspects of such criminal offences, detection of criminal offences and their traces, prosecution and trial of perpetrators of criminal offences, exclusion of persons from the procedure and assistance to the victims of criminal offences, and so as to enable the exchange of personal data with the competent*

[896] Orig. slo. Zakon o nalogah in pooblastilih policije, ZNPPol.

authorities of other countries for these purposes, the police shall collect from the suspect in each individual case data on his identity and DNA profile and save them in the record of DNA tests.

(5) During a pre-trial investigation concerning the criminal offences referred to in the act governing cooperation in criminal matters with EU Member States that allows the enforcement of a warrant for arrest and surrender regardless of double criminality, the police shall take fingerprints from the suspect in each individual case for the purposes of seeking suspects of these criminal offences, detection of criminal offences and their traces, prosecution and trial of perpetrators of criminal offences, exclusion of persons from the procedure or assistance to the victims of criminal offences. The fingerprints taken shall be kept in the record of fingerprinted persons, so as to enable the exchange of personal data with the competent authorities of other countries for the aforementioned purposes.

In addition to this general legal basis for the processing personal data by the police under PTPA, it needs to be highlighted that the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (ZVOPOKD)[897] supplements the relevant legal framework. This act relates to the protection of personal data processed by the police, state prosecutor's offices, the Probation Administration of the Republic of Slovenia, the Administration of the Republic of Slovenia for the Execution of Criminal Sanctions and other state bodies of the Republic of Slovenia, that are authorised to detect or prosecute criminal offenses or to execute criminal sanctions. It concerns the personal data processing for the purposes of the exercise of these powers. It also regulates the conditions for lawful and fair processing of personal data, procedures and methods of detecting and preventing unlawful interference with the rights of an individual to which personal data relates, methods of exercising his/her rights and transferring personal data to third countries and international organisations.

Personal data protection principles under the Article 5 of the ZVOPOKD are the following:

- legality, fairness and transparency (personal data are processed lawfully, fairly and transparently to the data subject);
- purpose limitation (personal data are collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes);
- minimum amount of data (personal data are relevant, relevant and limited to what is necessary for the purposes for which they are processed);
- accuracy and up-to-datedness (personal data to be accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that inaccurate personal data are deleted or corrected without delay, taking into account the purposes for which they are processed)
- limitation of the retention period (personal data to be kept in a form which permits identification of data subjects only for as long as is necessary to fulfil the purpose for which the personal data are processed, unless another retention period is laid down by law);
- integrity, confidentiality and availability (personal data are processed in a way that ensures adequate security of personal data, including protection against unauthorized or unlawful processing, against accidental loss, destruction, damage or loss of availability, by appropriate technical or organizational measures).

[897] OGRS, no. 177/2020.

The ZVOPOKD also provides provisions on personal data processing legality, especially in its Articles 6 and 7. The processing of personal data for the purposes of the above-mentioned competent authorities is lawful only:

a) if it is necessary and to the extent necessary to perform their tasks specified by law,

b) if the types of personal data, to which these personal data relate, the purpose of processing and

c) the retention period or the period for regular review of the need for retention is prescribed by law.

Competent authorities can process personal data of an individual who has given consent to for it. Irrespective of the mentioned purposes, the competent authorities are allowed exceptionally process personal data (taking into account the specific circumstances of the case) to protect the life or body of the data subject or other persons. In this case they have to provide the report to the Information Commissioner of the Republic of Slovenia.

The processing of specific[898] types of personal data is prohibited. Nevertheless, the processing is considered lawful if it complies with previous explanation (purpose, extent, retention period) and that the law provides conditions and measures to ensure adequate protection of human rights or fundamental freedoms of the data subject. At the same time, the processing is strictly necessary for the performance of the tasks of the competent authorities, or if the individual made them public or available, unless it derives from the communication within an inner circle of persons.

13.4.2. National Legislation on CSAM Database

Slovenia has prepared legislation for the establishment of a national database of materials for children who are sexually exploited, but the database itself is not yet in place and is being prepared.

Legislation on the national database of sexually exploited children is contained in PTPA[899]. The legal basis for establishing and maintaining the national database of CSAM and for the processing this type of data are provided in the following provision:

- **Police Records (Article 123, para. 1, 2[29] and 4 PTPA):**

  (1) The police shall manage and keep records of personal and other data collected and processed by police employees in the performance of police tasks.

  (2) The police shall keep the following records in connection with the exercise of police powers:

  […] 29. The record of materials relating to sexual exploitation of minors, […]

[898] According to the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (ZVOPOKD) *special types of personal data* means personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs or trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data relating to the health of individuals and in relation to an individual's sexual life or sexual orientation.

[899] Legal provisions are not official translation.

(4) The record referred to in point 29 of paragraph two of this Article shall contain collected, recorded and described materials of sexual exploitation of minors and is aimed at the implementation of procedures to determine the territorial, temporal, substantive and other circumstances of the emergence of these materials. The record shall also be aimed at the identification of persons featuring in the materials in order to trace and protect victims, detect suspects of criminal offences and gather information and evidence on acts of sexual exploitation of persons below 18 years of age.

Other provisions that regulate the national database of CSAM relate to the following questions:

- **Content of the records (Article 125, para. 1, point 29 PTPA)**

  (1) In addition to the data referred to in the preceding Article, additional personal data and other data or information, as provided by this Act, may be processed in particular records:

  …

  29. The record of materials relating to sexual exploitation of minors: photographs, audio and video recordings and other similar materials depicting or are connected to sexually exploited minors, technical data on the materials, description of contents of the materials, details of the criminal offence, data on the identification of the minor (date of identification, personal data referred to paragraph one of Article 124 of this Act) and data on the deletion of materials.

- **Common personal data in records (Article 124, para. 1 PTPA)**

  (1) The records referred to in the preceding Article may contain the following common personal data:

  - *full name,*
  - *data on birth (day, month, year and place),*
  - *personal identification number, or the number of the identity document for foreign citizens,*
  - *gender,*
  - *address of permanent and/or temporary residence,*
  - *identification code of the person kept in police records,*
  - *nationality.*

- **The right to access own personal data (article 127, para. 1, indent 1; para. 5 PTPA)**

  (1) Persons shall have the right to access their own data in the records referred to in:

  - *Points […] 29, […] of paragraph two of Article 123 of this Act immediately after the record is set up; […].*

  (5) The police shall refuse a request for a printout of data from the record referred to in point 29 of paragraph two of Article 123, except when such a request is filed by the court, state prosecutor's office or another authority in connection with the detection, prosecution or trial for a criminal offence against sexual inviolability of persons younger than 18 years of age.

- **Data retention period (Article 128, para. 1, indent 20; para. 3, sentences 2 and 4; para. 4 and 5 PTPA)**

  (1) The data in the records referred to in paragraph two of Article 123 shall be retained for the following periods:

  - *[20] in the record under point 29, until the identity of a minor is established and then for 60 years from the day the identity of that person is established; […].*

  (3) […] Access to data in the records under point 29 of paragraph two of Article 123 of this Act shall be allowed to the state authorities competent for the beginning, institution and implementation of the pre-trial investigation or criminal procedure in accordance with the regulations governing the criminal procedures and holders of public power in the area of social assistance when conducting procedures related to persons at risk on account of criminal offences against sexual inviolability. […] Competent state authorities shall be allowed access to other records only in order to perform their tasks provided by law.

  (4) If the identity of the injured person referred to in point 29 of paragraph two of Article 123 is known, he must be acquainted with the retention of data and the right to deletion referred to in paragraph five of this Article.

  (5) The deletion of data from the record referred to in point 29 of paragraph two of Article 123 of this Act before the expiry of the time limit for its retention is only possible on the basis of a written request of the person or his legal representative. Before the deletion the police shall inform the eligible person of the consequences of the deletion. By way of an exception, the police may suspend the execution of the request for deletion of data if the deletion may put the identification of another injured person at risk or if the deletion may obstruct the investigation of a criminal offence.

- **Data blocking (Article 129, para. 2, indent 11 PTPA):**

  (2) After the blocking, the data:

  - *in the records under points […] 29 of paragraph two of Article 123 shall be deleted; […].*

13.4.3. INTERPOL's ICSE and Europol's IVAS

Since 2015, Slovenia is connected to the INTERPOL's International Child Sexual Exploitation Images (ICSE) Database and has been active in it. The "ICSE database" is used in the fight against sexual exploitation and abuse of children, mainly for the victim identification purposes. This database is the image and video comparison database, into which CSAM are uploaded by the certified law enforcement experts worldwide.

Since 2016, Slovenia is added to the IVAS repository and has been active in it. The IVAS, maintained by Europol and operates at European level, stands for the Images and Videos Analytical System and is used similarly to the ICSE database.

13.4.4. Legal Basis for the Police to Exchange Personal Data Internationally

The legal basis for the international police cooperation also lies in provisions of the law that regulates police tasks and powers. Beside previously mentioned personal data protection measures, principles and laws, the Article 117 PTPA provides the legal basis for the transmission of personal data to foreign authorities and international organizations. Article 117 explicitly says:

> *(1) The transfer of personal data to a body of an international organization pursuant to an international agreement by which the Republic of Slovenia delegated the exercise of sovereign rights and the transfer of personal data to EU or European Economic Area Member States shall be carried out on the basis of a relevant international treaty, legal act or decisions of the international organization, or pursuant to the provisions of the laws implementing these legal acts or decisions.*
>
> *(2) The police may, if this is necessary for exercising police powers, provide personal or other data collected to authorities of other countries or international organisations to which the Republic of Slovenia has not transferred the exercising of a part of sovereign rights, at their request or on its own motion subject to effective reciprocity. The police may designate certain personal data as sensitive and limit the purpose of their processing.*
>
> *(3) Before personal data are passed to the authorities referred to in the preceding paragraph, the police must acquire guarantees that the country to which the data are being sent has a regulated personal data protection system and that the authority of a foreign country or international organisation will only use personal data for the purposes set out in this Act. The national supervisory authority responsible for the protection of personal data shall issue a decision on the adequacy of personal data protection in the third country or international organisation for cross-border data exchange.*
>
> *(4) The police must ensure that it is noted, in the record from which the data was taken, which personal data were passed on, when, to whom, for what purpose and on what grounds.*
>
> *(5) When providing data, the police must, if this is necessary in view of their content, specify how accurate, complete, updated and reliable they are, and request equal cooperation of authorities of other countries or international organisations in cross-border data exchange. In the processing of data and other documents received, the police and other users must comply with the restrictions imposed by the transmitting authority.*
>
> *(6) In the case of cross-border exchange referred to in the preceding paragraph, the personal data shall only be provided to law enforcement or similar authorities of other countries or international organisations that require them for operations or decision-making, if their processing is not inconsistent with the purposes referred to in Articles 1 and 4 of this Act. The authorities referred to in the preceding sentence must comply with the data processing restrictions imposed by the police based on the legal order of the Republic of Slovenia, in particular to ensure the protection of interests of proceedings, confidentiality of proceedings, privacy of persons or protection of the presumption of innocence or right to a fair trial.*

In general, the transmission and processing in this regard is possible based on a relevant international treaty, legal acts or decisions of international organizations or pursuant to the provisions of the laws implementing these legal acts or decisions. If it is necessary to exercise the police powers, they may provide personal or

other data to competent foreign authorities (usually law enforcement), at their request or on its own motion under the subject to effective reciprocity. The police may designate certain personal data as sensitive and limit the purpose of their processing. The police must ensure that the type, time, addressee, purpose and basis for the transmission of the data are properly recorded.

13.4.5. Police: Cross-Border Cooperation and Cross-Border Exchange

The National Slovenian Police uses both, European and international channels for cross-border cooperation and cross-border exchange of information. The explanations in this section are limited to the context of the GRACE project.

Legal basis was already provided in section 13.4.4, while in practise Slovenian National Police uses the Secure Information Exchange Network Application (SIENA), owned and managed by Europol. It is provided in secured environment for the exchange of information and it is essential for the secure and swift transmission of sensitive and restricted data. In addition, the Large File Exchange (LFE) solution offers and enables a secure exchange of files that exceed the size limit of the SIENA, when the need arises (for example sending an image of a hard drive or copy of a server).[900]

At international level, Slovenian Police, through Europol, co-operates with the National Centre for Missing and Exploited Children (NCMEC) in the USA that works closely with law enforcement officers in combating child exploitation. US based online service providers report the existence of the images and videos of sexually abused children (CSEM/CSAM) to US NCMEC, which further disseminate via Europol to several EU Member States for further processing and possible investigation. Slovenian Police are receiving these referrals via Europol.

Slovenian Police is a member of Europol since 2004. Furthermore, Slovenia became a member of the International Police Organization (INTERPOL) in 1992.

The National Central Bureau (NCB) for Slovenia and the Europol National Unit (ENU) are part of the International Police Cooperation Division under the Criminal Police Directorate[901] at the General Police Directorate within Slovenian National Police.

The NCB links the Police to its worldwide counterparts and plays a main role in preventing the country and surrounding region from serving international organized crime. One of the main INTERPOL information categories are crimes against children, especially combatting the sexual exploitation and abuse of children.

Slovenia and Slovenian Police are cooperating and collaborating with countries in the Western Balkan region due to its geo-strategic position and common history. These provide the ability to work more closely with the partners in the region on more intensive bi- or multi-lateral level.

[900] EUROPOL Intelligence: The Secure Information Exchange Network Application (SIENA), https://www.europol.europa.eu/annual_review/2015/intelligence.html.

[901] Orig. slo. Sektor za mednarodno policijsko sodelovanje, Uprava kriminalistične policije, Generalna Policijska Uprava (SMPS UKP GPU).

13.5. Electronic Evidence

The Criminal Procedure Act (CPA) contains several provisions, which indirectly define electronic evidence as "information/data in an electronic format." As an example, para. 1 of Article 219.a of the CPA provides:

> *(1) A search of electronic and associated devices, and electronic data storage device (electronic device) including over the network connected and accessible information systems where data is stored, may be conducted for the purpose of obtaining information in an electronic format when there are grounds for a suspicion a criminal offence was committed and it is likely that the electronic device contains electronic information:*
>
> - *on the basis of which it would be possible to identify the suspect or accused, detect or apprehend traces of the criminal offence that are important for criminal proceedings; or*
> - *which may be used as evidence in criminal proceedings. [...]*

Moreover, the following provisions of the Electronic Business and Electronic Signature Act (EBESA)[902] are also relevant in terms of defining the scope and content of the term electronic evidence:

- *"information/data in an electronic format* is data/information which is formatted, saved, sent, received or exchanged electronically" (Article 2 EBESA);
- *"data/information in electronic format* may not be denied validity or evidentiary value based on the fact that it is in an electronic format" (Article 4 EBESA).

In addition, Slovenia ratified by law the Convention on Cybercrime (Budapest Convention), which among others defines:

- "computer data" as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function (Article 1(b) Budapest Convention); and
- "traffic data" as any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service (Article 1(d) Budapest Convention).

It is important to acknowledge the specific terminology used in Slovenian legal environment – the so-called *list/catalogue of offences*. These are the criminal offences, prescribed in the Criminal Code and specifically listed in the para. 2, Article 150 of the CPA that are of the serious nature due to their gravity and consequences. Some of these criminal offenses are:

- Acquisition of persons under the age of fifteen for sexual purposes under Article 173a,
- Abuse of prostitution under Article 175,

[902] OGRS, no. 98/2004 Official Consolidated Text (orig. slo. Zakon o elektronskem poslovanju in elektronskem podpisu, ZEPEP).

- Display, production, possession and distribution of pornographic material under Article 176,
- Extortion under Article 213,
- Criminal association under Article 294 and
- Other offenses, if they are punishable by eight or more years' imprisonment (e.g. sexual assault on a person under the age of fifteen under Article 173).

Since the list or catalogue is quite extensive and it would be superfluous to represent the whole, the decision was made to introduce only those that are in the context of the GRACE project and criminal trends in CSE area.

13.5.1. Possible Measures

All measures that are available in Slovenian national legislation regarding obtaining and securing electronic evidence for the purposes of identifying the suspect or accused, detecting or apprehending traces of the criminal offence that are important for criminal proceedings and which may be used as evidence in criminal proceedings are also available under International Judicial Cooperation via a Mutual Legal Assistance (MLA) request or an European Investigation Order (EIO). These would among others be:

- Expedited preservation of stored *computer data*;
- Expedited preservation and partial disclosure of *traffic data*;
- Production order (both for physical persons and for service providers);
- Search and seizure of stored *computer data*;
- Real-time collection of *traffic data*;
- Interception of *content data*.

It should be noted, however, that installation of state-sponsored *trojan* software to users' devices for collecting and gathering of electronic evidence (at the source) is not allowed. Additionally, it should also be noted that while the use of IMSI-Catcher devices as a means of intercepting *traffic data* has been implemented in the last amendments to the Slovene Criminal Procedure Act 2019 (CPA-N). On the other hand, the provisions regarding so called IMSI-Catcher devices are currently under constitutional review by the Slovene Constitutional Court[903] and pending its decision the relevant articles are suspended (i.e. IMSI-Catchers are currently not allowed to be used either).

[903] See Constitutional court decision U-I-144/19-16 from 4. 7. 2019, available at: https://www.us-rs.si/wp-content/uploads/2020/05/u-i-144-19.-.sklep_.pdf.

13.5.2. Procedures for Obtaining Electronic Evidence

Presented are national and international procedures.[904]

13.5.2.1. National Procedures

Depending on how strongly a specific measure in connection to gathering and collecting of electronic evidence impacts and interferes with constitutionally guaranteed freedoms and rights, CPA provides for specific conditions and evidentiary standards for each of the available measures.

In general, depending on the severity and intrusiveness of the measure, Slovenian legislator limited the availability of the specific measures by prescribing:

1. Who may decide and order a specific measure (police/prosecutor/judge);

2. Different applicable catalogues of crimes for which specific more intrusive measures are available;

3. Specific evidentiary thresholds for using a specific measure (these are, listed in order from lower to higher threshold:

    a. reasons for suspicion (orig. slo. razlogi za sum),

    b. grounded reasons for suspicion (orig. slo. utemeljeni razlogi za sum),

    c. reasonable suspicion (orig. slo. utemeljen sum);

4. Limiting the time duration of a specific measure;

5. Limiting the duration of the "gag order" prohibiting disclosure by the operator/service provider to the person whose data is being processed that his (data) was transmitted to the authorities.

With respect to disclosure of various data, for example, there are different regimes for who may order *disclosure of subscriber data information*, that is the data relating to the owner or user of a specified electronic device and who may order *disclosure of traffic data*. As a "golden" general rule, if the service provider given the input information (e.g. IP address) needs to process other traffic data to identify the subscriber (e.g. in cases of dynamic IP addresses) it will always be a judge who decides on the production order. In cases where processing traffic data is not necessary to identify the subscriber/user of the electronic device, the police or the prosecutor can also order the service provider to identify and hand over subscriber information (but not the traffic data as well). The described normative framework is the result of constitutional guarantees that interception of communication can only be ordered by a judge. The Slovenian constitutional court follows the doctrine that (transactional) traffic data even though not being content of communication itself is such information which is, given its informative value, its functional and constitutional equivalent (i.e. traffic data can be even more revealing and a greater intrusion regarding to the constitutional right to communication privacy than the content of the communication itself. The doctrine was further developed by the constitutional

[904] This sub-chapter was adapted from the European Judicial Network website, Slovenia: https://www.ejnforum.eu/cp/e-evidence-fiche/369/0#.

court[905] in later decisions, meaning that (transactional) *traffic data* enjoys the same protective constitutional regime as does the content of the communication itself (court order is required).

Given that *temporary freezing/securing of (traffic) data* on its own is a less intrusive preliminary measure (as it does not involve possible later production of the *frozen (traffic) data* which can only be ordered by a judge), police and prosecutors can demand the so called "data freeze" themselves (Article 149.e of the CPA). This measure is intended to prevent erasure of electronic evidence, whether individuals or legal entities on electronic devices or by the operators of electronic communications or websites store them. It can be demanded for a list of criminal offences for the purposes of discovering, prevention or proving such offences or for discovering the perpetrators of such offences.

The standard of reasons for suspicion (orig. slo. razlogi za sum) that such offence has been committed or is to be committed or is organized has to be met. It also has to be shown that it is likely that the data in question will otherwise be lost or altered by the time of the production order is issued by the court. The *data freeze* can last for 30 days from the service of the demand until the receipt of the court order for obtaining such data and can be prolonged for another 30 days. After max 60 days the preservation of the data is abolished, if the court order is not obtained.

The *seizure and search of electronic device* is possible (Article 219.a and 223.a of the CPA), if grounded reasons for suspicion (orig. slo. utemeljeni razlogi za sum) exist that the criminal offence was performed and probability exists that there are electronic data on the electronic device. This measure can be carried out on the basis of the individual's consent or on the basis of a court order.

The so-called *subscriber data* can be obtained by the police, state prosecutor or court based on reasons for suspicion (orig. slo. razlogi za sum) that such offence has been committed or is to be committed or is organized (Article 149.č of the CPA). According to the CPA, the service provider is not allowed to inform the user, subscriber or third person that the data has been or will be provided for a period of 24 months after the data has been provided. The judge can order a shorter duration of the "gag order" in any subsequent production order where the initial *subscriber data* was used and can also extend it by 12 months, but only twice.

The so-called *traffic data* (Article 149.b of the CPA), that is the data regarding the communication of the suspect, victim or person for whose communication it is reasonable to suspect that could bring to identification of the suspect, can be obtained for a list of criminal offences, if there are reasons for suspicion (razlogi za sum) that such offence has been committed or is to be committed or is organized. *Traffic data* can be obtained on the basis of the court order only. In specific cases defined by the law this data can also be collected in real time on the basis of the court order (Article 149.c of the CPA).

The CPA also provides for the possibility of:

- *monitoring of electronic communications using listening and recording devices* and the control and protection of evidence on all forms of communication transmitted over the electronic communications network (real-time interception of communications);

[905] See the decision of the Constitutional Court of the Republic of Slovenia no. Up-106/05, from 2. 10. 2008, available at: http://www.us-rs.si/documents/bf/0c/up-106-052.pdf and among other decisions of the Constitutional Court of the Republic of Slovenia, no. U-I-65/13. From 3. 7. 2014, available at: https://www.us-rs.si/odlocba-ustavnega-sodisca-st-u-i-65-13-z-dne-3-7-2014/.

- *control of the computer systems of banks or other legal entities* which perform financial or other commercial activities (real-time monitoring of bank transactions);
- *listening to and recording of conversations* with the permission of at least one person participating in the conversation.

These measures are possible for the list/catalogue of offences if grounded reasons for suspicion (orig. slo. utemeljeni razlogi za sum) exist that a certain person has committed, is committing or is preparing to commit or organizes such criminal offence and there is reasonable suspicion (orig. slo. utemeljen sum) that a certain communication means is being used for this offence and there are no other, milder measures that can be used for obtaining evidence (proportionality test). These measures can be obtained on the basis of the court order only.

13.5.2.2. International Procedures

- **Slovenia as requesting/issuing state:**

In general, national procedures for obtaining e-evidence from abroad (i.e. when Slovenia is requesting or issuing state) are the same as obtaining e-evidence within Slovenia, which means that the same evidentiary standards apply, measures listed above apply for the same lists of offences and the same procedure is applied. If the evidence is to be obtained from abroad, the authority that is competent to issue the decision (e.g. court or prosecutor) is also competent to use the relevant international instrument, make the MLA request (or EIO) that is compliant with the international instrument used and send it to competent authority abroad.

Specifically regarding the *monitoring of electronic communications*, the Cooperation in Criminal Matters with the Member States of the European Union Act[906] (Article 77.k) provides for the obligation to notify the other EU Member State in accordance with Art. 31 of the EIO Directive, when monitoring of the electronic communication of a person is ordered in Slovenia, and the person is currently in that state, yet *no technical assistance* is required from this other state. Notification can be sent in advance or ex post, depending on the actual knowledge of the whereabouts of the person.

The national court can also issue an European Investigation Order (EIO) to monitor telecommunication devices in other Member State, whose *technical assistance is needed* in accordance with Art. 30 of the EIO Directive (Article 77.i of the Cooperation in Criminal Matters with the Member States of the European Union Act). National court can also ask the other Member State and its body to make the transcript of the tape or to decrypt it, if the latter agrees with it.

- **Slovenia as requested/executing state:**

With EU Member States: In accordance with national legislation (Art. 65 and 66 of the Cooperation in Criminal Matters with the Member States of the European Union Act) the competent authority executes EIO requesting e-evidence in the same manner and under same conditions as the requested measure is ordered by national

[906] OGRS, no. 48/2013, 37/2015, 22/2018 and 94/2021 (Orig. slo. Zakon o sodelovanju v kazenskih zadevah z državami članicami Evropske unije - ZSKZDČEU-1).

authority, i.e. the manner of execution of the requested measure and appropriate measures in accordance with national law (Criminal Procedure Act) are ordered by the authority that orders measure in the national proceedings (court). In cases when issuing Member State asks for the measure to be ordered in a manner provided by the legislation of that country, the competent authority in Slovenia orders so if such a manner is in accordance with the fundamental principles of the national legal system.

Specifically regarding the *monitoring of electronic communications*, Cooperation in Criminal Matters with the Member States of the European Union Act (Article 77.k) regulates the situation of notification received by the other EU Member State in accordance with Art. 31 of the EIO Directive, when *monitoring of the electronic communication* of a person is ordered in another Member State, and the person is currently in Slovenia, yet *no technical assistance* is required from Slovenia. Competent authority in Slovenia for receipt of such notification from another Member State is District Court in Ljubljana. This court has obligation to inform the authority that sent the notification if it does not allow the monitoring on the territory of Slovenia or that monitoring should be terminated because such measure would not be allowed in a similar domestic case. The court has to inform the authority of another Member State in 96 hours.

If the national court is asked to execute EIO on the monitoring of telecommunication it does so, if the conditions of the Slovene Criminal Procedure Act are respected (Article 77.j. of the Cooperation in Criminal Matters with the Member States of the European Union Act). The requesting state can monitor communications directly (if technically that is possible) or the nationally monitored communications can be later provided to it.

With non-EU states: in accordance with national legislation (Art. 516 of the Criminal Procedure Act) the authority competent to order the measure requested by a foreign authority decides about the permissibility of the measure and the manner of enforcement in accordance with national legislation and international agreements. In cases when requesting country asks for the measure to be ordered in a manner provided by the legislation of requesting country, the competent authority in Slovenia may order so if that is in accordance with the fundamental principles of the national criminal proceeding.

- **Channels of communication:**

With EU Member States: the general rule is direct cooperation between competent judicial authorities, in accordance with EIO Directive, except for Denmark and Ireland (channel of communication is central authority);

With non-EU states: The Ministry of Justice of the Republic of Slovenia acts as the Central Authority. Provisions of relevant international instruments[907] providing for the possibility of direct communication apply in relation to the states that have ratified relevant instruments. Communication via police channels is used in cases provided for in the relevant international instrument that is used in a specific case. Direct communication between judicial authorities and communication through police channels is possible also when no international instrument applies under the condition of reciprocity (Article 515 of the CPA).

[907] E.g. European Convention on Mutual Assistance in Criminal Matters 1959 and Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters 2001.

- **Definition of data category**

Subscriber data are indirectly defined (Article 149.č of the CPA) as data regarding the owner or user of a certain communication device or of a service of information company or data about the existence and content of his contractual relationship with a service provider. The content of the contractual agreement between an individual and the operator is furtherly defined in Electronic Communications Act (ECA).[908] The contract should for example include information on the offered service and time of its duration.

Traffic data are defined as any data processed for the purpose of transmission of communication through an electronic communication network or because of its billing (point 55, Article 3, ECA). Typical traffic data are the time and duration of the telephone call between two mobile phones.

Traffic data can be acquired, if the threshold of reasons for suspicion that a criminal offence from the catalogue (which is identical to the one for secret surveillance – i.e. "following" of the suspect) was committed is fulfilled. The mentioned catalogue consists of all *ex officio* prosecuted criminal offences, for which prison sentence of five or more years is prescribed in the Criminal Code as well as other individually listed criminal offences, which were chosen on the basis of their nature or gravity of the prescribed sanction.

In narrowly defined cases, such as thefts of the mobile phones (i.e. criminal offences, which are prosecuted ex officio and for which at least one year of prison sentence is prescribed), the Criminal Procedure Act allows for gathering of traffic data in "real time", in case that the threshold of reasons for suspicion is shown in the request for the court order.

Content data are not specifically defined in the law. In general, the threshold of specifically grounded reasons for suspicion that a criminal offence, which is prosecuted *ex officio* and is included in the catalogue must be fulfilled (this covers also all such criminal offences for which the prison sentence of at least eight years is prescribed in the Criminal Code).

13.5.3. Use of Crawlers

The use of the search robots is not mentioned in Slovenian legislation. It is believed that their use is not allowed, since they are not prescribed in the law.

[908] OGRS, no. 130/2022 (Orig. slo. Zakon o elektronskih komunikacijah – ZEKom-2).

14. Country Report on Cyprus

This Country Report aims to outline the legal framework regulating the fight of Law Enforcement Agencies (LEAs) against Child Sexual Exploitation Materials (CSEM) in Cyprus. A special focus is given to the use of tools and devices benefiting from the capabilities of machine learning and/or artificial intelligence (AI).

14.1. Victims' Rights

"In Cyprus, criminal proceedings begin with a police inquiry into the crime. Once the inquiry is finished, the case is referred to the Attorney-General of the Republic who decides whether to initiate criminal proceedings. If there is sufficient evidence against the alleged perpetrator, the Attorney-General will refer the case to court for trial. Once it has examined the evidence gathered, the court will decide whether the defendant is guilty and either sentence or acquit him/her".[909]

This section presents an overview of the legal rights and claims available to victims of Child Sexual Exploitation (CSE).

14.1.1. Criminal Procedure Rights (Updated for Legal Report v2)

Rights and claims available to victims of CSE are provided in the Law on the Prevention and Control of Sexual Abuse, Child Sexual Abuse and Child Pornography (Law 91(I)/2014),[910] the Law on the Establishment of minimum standards on the rights, support and protection of victims of crime (Law 51(I)/2016)[911], the Law on Domestic Violence (Prevention and Protection of Victims), (Law 119(I)/2000) and the Law on the Prevention and Combating of Trafficking and Exploitation of Persons and the Protection of Victims, (Law 60(I)/2014).[912]

Law 51(I)/2016 grants victims of crime in general, and Laws 91(I)/2014, 119(I)/2000, 60(I)/2014 grant CSE victims in particular, various rights. At first, it must be noted that according to Article 5 of Law 51(I)/2016, the police has to take all appropriate measures in order to help victims to understand and be understood. The police must make sure that it uses plain and intelligible language in its communication. Furthermore, the victim has the right, during his/her first communication with the police to be accompanied by a person of his/her

[909] European E-Justice, Rights of victims of crime in criminal proceedings – Cyprus, https://e-justice.europa.eu/content_rights_of_victims_of_crime_in_criminal_proceedings-171-CY-en.do?idTaxonomy=171&idCountry=CY&plang=en&init=true&removebanner=true

[910] Law 91(I)/2014 transposes into national law, Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335.

[911] Law 51(I)/2016 transposes into national law, Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, OJ L 315.

[912] Law 60(I)/2014 transposes into national law, Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, OJ L 101.

choice, save where this is detrimental to his/her interests or to the course of the proceedings.

Additionally, the same Laws grant victims of crime in general and CSE victims in particular, multiple information rights. More specifically a victim of CSE has the right, after the crime has occurred, but before this is reported, to be informed, *inter alia*, about:

- the support he/she can have including, where relevant, basic information regarding access to medical support, any specialist support, including psychological support, and alternative housing (Article 6(1)(a) of Law 51(I)/2016, Article 36(1)(a) of Law 91(I)/2014), Article 32(1)(b) of Law 60(I)/2014;
- the procedures for reporting a crime and the role of the victim in the context of those proceedings (Article 6(1)(b) of Law 51(I)/2016, Article 36(1)(c) and (d) of Law 91(I)/2014), Article 32(1)(c) and (d) of Law 60(I)/2014;
- the procedure and conditions under which protection is provided, including protection measures, (Article 6(1)(c) of Law 51(I)/2016), Article 36(1)(e) of Law 91(I)/2014), Article 32(1)(e) of Law 60(I)/2014;
- the procedure and conditions under which compensation may be claimed, (Article 6(1)(d) of Law 51(I)/2016), Article 36(1)(g) of Law 91(I)/2014), Article 32(1)(g) of Law 60(I)/2014;
- the procedure and conditions under which the victim is entitled to interpretation and translation services, (Article 6(1)(e) of Law 51(I)/2016);
- the procedure and conditions under which expenses incurred as a result of participation the criminal proceedings can be reimbursed, (Article 6(1)(i) of Law 51(I)/2016);
- the procedures available for filing complaints where the victim rights are not respected by the department involved, (Article 6(1)(g) of Law 51(I)/2016);
- the contact details of the Police officer handling the case, for communication purposes (Article 6(1)(h) of Law 51(I)/2016).

Furthermore, a victim of CSE has the right, after reporting a crime, to be informed, *inter alia*, about:

- any justified decision not to proceed with or to end an investigation or not to prosecute the offender, (Article 8(1)(a) of Law 51(I)/2016), Article 36(2)(a) of Law 91(I)/2014));
- the time and place of the trial, and the nature of the charges against the offender, (Article 8(1)(b));
- any final decision that has been issued by the court (Article 8(1)(c) of Law 51(I)/2016), Article 36(2)(c) of Law 91(I)/2014), Article 32(2)(c) of Law 60(I)/2014;
- details regarding the course of the criminal proceedings (Article 36(2)(b) of Law 91(I)/2014 and Article 32(2)(b) of Law 60(I)/2014). Yet in exceptional circumstances, where the proper handling of the case may be adversely affected by disclosing such information, it may be withheld following a reasoned opinion of the Attorney General of the Republic of Cyprus, (Article 8(1)(d) of Law 51(I)/2016);
- his/her right to be informed of the date if the person remanded in custody, prosecuted or convicted for the crime related to him/her is released or has escaped as well as of any measures that have been decided for his/her protection, in case of the release or escape. Such information may be withheld if

there is a potential or established risk of harm for the offender or if the victim requests in writing not to receive this information, (Article 8(3) of Law 51(I)/2016 as amended by Law 36(I)/2022).

Furthermore, victims of CSE are entitled to free legal aid, (Articles 37(3) and 40, Law 91(I)/2014 and Article 32(1)(f) and Article 33 of Law 60(I)/2014).

14.1.2. Witness Protection (Updated for Legal Report v2)

"As it is widely accepted, witness protection is fundamental to an effective criminal legal system. For this purpose [for Cyprus] the Protection of Witness Law of 2001, otherwise known as Law 95(I)/2001, regulates the matter fully".[913]

More specifically, according to Law 95(I)/2001, a court in a criminal case, in order to protect vulnerable witnesses, can declare a person as a "witness that requires help" ex officio or under application filled at any stage of the process. More specifically a witness in criminal proceedings may be declared as a person that requires help if, *inter alia,* at the time of the hearing, is under the age of eighteen (Article 3(1)(a)), or the court considers that the testimony to be given by the witness might be affected because of his/her reduced mental and social adaptability, (Article 3(1)(b)), or the witness suffers from a physical weakness or disability (Article 3(1)(c)). Furthermore, Article 3(4) establishes that when a victim of an offence provided by the Law on Domestic Violence as well as the Law on the Prevention and Combating of Trafficking and Exploitation of Persons and the Protection of Victims, (Law 60(I)/2014), is a witness in criminal proceedings, then that witness is considered a "witness that requires help" unless otherwise stated by the witness himself/herself.

The measures available to a court to implement in order to protect a "witness that requires help", these are set out in Part III of Law 95(I)/2001. In particular, the court can order, *inter alia*, that a) all or part of the case be heard behind closed doors (Article 5(1)(a)), b) the testimony of a "witness that requires help" is given in the absence of the defendant, provided that he is informed of the content of the said testimony and his right to cross-examination is not affected (Article 5(1)(b)), c) there is a placement of special separation system (Article 5(2)(a), d) a closed electronic circuit system is to be used, to enable the said witness not to be visible by the defendant (Article 5(2)(b)), and e) audio-visual testimony is accepted as evidence under certain conditions, including his obligation, if requested, to appear before the court for cross-examination (Article 9).[914]Furthermore, according to Article 15, especially for victims of an offence, regulated by the Law on Domestic Violence, as well as by the Law on the Prevention and Combating of Trafficking and Exploitation of Persons and the Protection of Victims, the publication of his/her name as well of his/her testimony, or part of it, is strictly forbidden.

Furthermore, Article 16, of Law 95(I)/2001, authorizes the establishment and operation, under the control and

[913] Council of Europe, Committee of Experts on Terrorism (CODEXTER) Profiles on Counter-Terrorist Capacity, Cyprus, May 2011 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806 40f00

[914] The right of a victim of domestic violence, to provide audiovisual testimony is additionally regulated by Article 9 of Law 119(I)/2000.

supervision of the Attorney General, of a Scheme for the Protection of Witnesses. A witness is admitted, upon the Attorney-General's decision, provided that the conditions set out in Article 18 are fulfilled. Under this Scheme, various protective measures may be taken, so as to encourage and safeguard the testimony of vital witnesses who would have otherwise been at risk. Such protective measures may be extended, if needed, to protect additionally a witness's family. In detail, these protective measures, found in Article 17, include *inter alia* guarding or escorting the witness and his/her family, moving the witness and his/her family to another town or village or, even, abroad and the change of identity of the witness or any of his/her family members.

14.1.3. Compensation and Assistance for Victims of Sexual Offences

The issue of compensation for victims of sexual offences is provided in the Law on Prevention and Control of Sexual Abuse, Sexual Exploitation of Children and Child Pornography (Law 91(I)/2014) that, as aforementioned, transposes Directive 2011/93/EU, into Cypriot law.[915] More specifically, according to Article 39(1), victims have a right to file a claim for damages against all parties liable, for all the crimes, as well as for all human rights violations, that have been committed against them. The offender bears the respective civil liability to pay compensation for all specific or general damages incurred by the victims, including any arrears owed to the victim(s) as a result of their forced employment. Article 39(3) provides for the parameters that must be taken into consideration, by the court in order to determine the amount of compensation for general damages. According to Article 39(5) in case of death of the victim, the parents or the beneficiaries of the parental care or the administrator of his/her property have an enforceable right to compensation.

14.2. Data Protection

Regarding crime investigations by LEAs, personal data is protected in accordance with a specific legal framework. According to Art. 2(2)(d) General Data Protection Regulation (GDPR or Regulation),[916] the Regulation does not apply to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In detail, according to Recital 19 GDPR, personal data processed by public authorities under the GDPR, should, when used for such purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680,[917] otherwise known

[915] See footnote 2.

[916] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119.

[917] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

as the Law Enforcement Directive. The Law Enforcement Directive was transposed into Cypriot law in March 2019, through the Law on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties and for the free movement of such data (Law 44(I)/2019).

14.2.1. General Principles for Processing Personal Data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties and for the free movement of such data

According to Article 5(1) of Law 44(I)/2019 the controller, shall ensure that personal data are:

a) processed lawfully and fairly;

b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.[918]

14.2.2. Specific Regulations for Processing Data by the Police (Updated for Legal Report v2)

Apart from Law 44(I)/2019 that functions as an umbrella legislative instrument regarding the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences,

penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119.

[918] Yet Law 44(I)/2019 imposes various restrictions on the processing of personal data by LEAs and inevitably fetters LEAs' power to investigate crime.

additional powers are conferred upon members of the Cyprus Police regarding this issue, that can be found in various other national legislative acts. Of the most important of these legislative acts for the context of CSE crime are:

The Police Law of 2004 (Law 73(I)/2004) confers upon the members of the Cyprus Police specific powers regarding the investigation of offences. Apart from traditional powers conferred upon police officers, this Law ascribes, to certain categories of police officers,[919] the power to collect data such as fingerprints and DNA samples. One needs to note that no reference to Big Data is made in this Law. In detail, Article 25 of Law 73(I)/2014, provides that:

(1) Any member of the Police with the rank of Sergeant or higher may collect or arrange for the collection from any person who is in legal custody or who is subject to police surveillance, for the purposes of registration, comparison, identification and generally for purposes of investigating any offence:

(a) measurements, photographs, fingerprints, palm and sole prints, graphic specimens, nail clippings, hair, saliva samples, foreign matter residues in the body of any of these persons with his consent or by order of the Court, if he does not consent.

(b) with the assistance of a medical officer, blood and urine samples of any of these persons with his consent or by order of the Court, if he does not consent.

(2) If the person to whom the information obtained under subsection (1) relates is not charged with a misdemeanor in court or if he is dismissed without charge or acquitted by the Court and is not subject to a prior conviction for a criminal offence, then all records of measurements, photographs, fingerprints and palm and footprints and any negative copies of these photographs or photographs of these fingerprints shall be destroyed immediately or delivered to the person to whom they relate.

The European Investigation Order in Criminal Cases Law (Law 181(I)/2017), transposes Directive 2014/41/EU into national law.[920] This Directive aims to foster effectiveness and expedience in the gathering of evidence in criminal proceedings and governs among others cross border secret investigations and interception of telecommunications. Article 21 of Law 181(I)/2017, reads that, personal data are protected and may only be processed in accordance with the Law Enforcement Directive. Furthermore, according to the same Article, access to such data shall be restricted, without prejudice to the rights of the data subject. Only authorised persons may have access to such data.

The Law on the Retention of Telecommunications Data for the Investigation of Serious Criminal Offences (Law 183(I)/2007), that transposes into national law Directive 2006/24/EC,[921] provides for the retention and police access to subscriber location and traffic data for the prevention, investigation and prosecution of serious crimes. Before moving on to examine the powers ascribed to the Cyprus Police by this Law, one needs to have

[919] Sergeant, Inspector, Chief Inspector, Superintendent B', Superintendent A', Chief Superintendent, Assistant Chief of Police.

[920] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130.

[921] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105.

a look at Directive 2006/24/EC. Interestingly the Court of Justice of the European Union (CJEU) in its landmark decision in Case, C-293/12, *Digital Rights Ireland Ltd*, of 8 April 2014 declared this Directive invalid on the grounds that it contravened Articles 7 and 8 of the EU Charter of Fundamental Rights. As Markou has argued, "this blatant rejection of the Data Retention Directive by the CJEU did not however prevent the Cyprus Supreme Court from stating that it had no effect on the national data protection legislation, which remained in force as national law (or part of the national legal order).[922] As a result, the Cypriot Court have thus continued upholding court orders allowing access to retained data based on the provisions of Law 183(I)/2007. This important issue is currently pending before the Cyprus Supreme Court and it remains to be seen whether there will be, after all, an alteration of the national legislative framework.

The legitimacy of specific articles of Law 183(1)/2007 was yet examined by the Cyprus Supreme Court in the *landmark Civil Application Case No. 97/2018,* otherwise known as the *Hadjioannou case,* on 27 October 2021.[923] In detail, a group of applicants challenged, in the Supreme Court, district court orders which had authorised access to their telephone data in the course of police investigations. The applicants argued that the data that the Cyprus Police was seeking to access had been unlawfully retained, because Law 183(I)/2007, which provided the legal basis for the retention, did not comply with the EU Charter of Fundamental Rights and CJEU related case law, for permitting the general and indiscriminate retention of data and location.[924] The applicants further argued that the safeguards contained in the Law, as regards access to retained data did not meet the criteria found in Council Directive 2002/58/EC as well as in the rulings of the CJEU in Cases, C-203/15 and C-698/15 *Tele2Sverige* and *Watson* as well as in Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net.* The Supreme Court concluded, in plenary, by a 7 to 6 majority, that Articles 3, 6 - 10 and 13 of Law 183(I)/2007 infringe Directive 2002/58/EC and related CJEU case law. Despite this important outcome, no amendment of the national data retention legislation has taken place up to now.

Interestingly, in the very recent case, *Civil Application Case No: 124/2022*,[925]decided on 14 February 2023, the Supreme Court ruled in favour of the retention of the IP addresses of internet users for the purpose of investigating online criminal offences. In detail, as part of an investigation, into a serious child sexual exploitation case, the Cyprus Police secured a court order requiring certain internet service providers to disclose the details of the user of a specific IP address, which was linked to the possession and distribution of illegal sexual exploitation material. The suspect filed a petition with the Supreme Court for the issuance of a privileged prerogative writ, that of Certiorari, seeking the annulment of the aforementioned order. The lawyer of the applicant argued that the issuance of the contested order was based on articles 3, 6 - 10 and 13 of Law 183(1)/2007, that had been ruled unconstitutional by the majority of the Supreme Court in the *Hadjioannou case*, since they violated fundamental human rights. The Supreme Court, rejecting this request, sided with the Advocate's General argument, who referred to CJEU C-793/19, *SpaceNet* case, stating that the general and

[922] Christiana Markou, Data Retention in Cyprus in the Light of EU Data Retention Law In Zubik and others (eds), European Constitutional Courts towards Data Retention Laws, (Springer, Springer Nature Switzerland, 2021) pp.85-99.

[923] http://cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_1/2021/1-202110-97-18PolAitEtc.htm&qstring=%E4%E9%E1%F4%E7%F1%E7%F3%2A%20and%20%F4%F9%ED%20and%20%F4%E7%EB%E5%F0%E9%EA%EF%E9%ED%F9%ED%E9%E1%EA%2A%20and%20%E4%E5%E4%EF%EC%E5%ED%2A

[924] https://fra.europa.eu/en/caselaw-reference/cyprus-supreme-court-civil-applications-concerning-telephone-data-no-9718-12718

[925] http://www.cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_1/2023/1-202302-124-22PolAitApof.htm&qstring=IP%20and%20address

indiscriminate retention of the IP addresses of all internet users is legal, as it is the only means of investigation that makes it possible to identify a person who has committed a serious offence through the internet. The Supreme Court, distinguished the facts of this case, with that of *Hadjioannou*, in that in the latter, the Court, did not examine, in principle, the compatibility of the contested provisions of Law 183(I)/2007 with EU legislation and case law on IP addresses, let alone with an emphasis on CSE offences, since those orders were linked to the retention of alternate forms of telecommunications data. The Supreme Court, finally ruled that the contested Articles, of Law 183(1)/2007, are not incompatible with EU law, explaining that they aim at combating serious crimes such as child pornography, and impose on telecommunication service providers the general and indiscriminate retention of IP addresses for a minimum of six months.

After reporting these interesting recent judicial outcomes, one can find, below, the powers ascribed to the Cyprus Police by the national legislation that remain, valid, up to now.

The Cyprus Police has increasingly been securing data access orders in relation to child pornography offences on the basis of this Law based on a previous court order (as required in Article 4). Every service provider, upon presentation of such a court order issued or a letter accompanied by the approval of the Attorney General of the Republic, in accordance with the provisions of Article 4, is obliged to make available, immediately and without any unjustified delay, to the police investigator all data specified in the relevant order or letter, (Article 5). Every service provider, has the obligation to retain specific data necessary a) to trace and identify the source of a communication, b) to identify the destination of a communication, c) to identify the date, time and duration of a communication, d) to identify the type of communication, e) to identify users' communication equipment or what purports to be their equipment and f) to identify the location of mobile communication equipment (Articles 6 – 11). Law 183 (I)/2007 and the data access court orders issued on its basis are often challenged before the Cypriot courts for violating human rights. This is considered a very serious problem for LEAs and the matter, as aforementioned, is currently pending before the Cyprus Supreme Court, which is expected to decide on the future of data retention in Cyprus. Furthermore, the Law on Privacy of Communication (Interception of Conversations and Access to Recorded Content of Private Communication) (Law 92(I)/1996), allows for the monitoring of a person's telecommunications, and access to the content of such communications, only after a court order is secured and for specific offences listed in the Cyprus Constitution. The list includes child trafficking as well as offences relating to child pornography.

14.3. Electronic Evidence

According to the Council of Europe Guidelines, ""Electronic evidence" means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network".[926]

In Cyprus, electronic evidence is covered, by Evidence Law, otherwise known as Chapter 9, which functions as the legal foundation, covering the general principles of this area of law that follow English common law (yet as applied in 1914!), as well as by the case law of the Supreme Court of Cyprus. Until 2004, hearsay evidence

[926] Council of Europe (2019) Electronic evidence in civil and administrative proceedings, https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

was deemed inadmissible by the Cyprus Courts. Since the passing of the Evidence (Amendment) Law (Law 32(I)/2004), as a general rule, hearsay evidence shall not be excluded from any court procedure merely because it is hearsay. According to Article 21(2) of Law 91(I)/2014,[927] without prejudice to the provisions of section 10 of the Evidence Law, a complaint by a victim to*, inter alia*, any police officer, social service worker, psychologist, psychiatrist or teacher shall constitute competent evidence. Furthermore, evidence of a victim given to an expert shall be considered as competent evidence. According to Article 17(1), of Law 119(I)/2000, where a minor, during his/her examination by a psychiatrist or psychologist mentions that he/she has been ill-treated by any person, the testimony of the psychiatrist or psychologist may be admissible in Court as an exception to the rule against hearsay. Yet, according to Article 17(2) of the same Law, the Court shall not convict any person upon such evidence unless such evidence is corroborated in material issues by other independent evidence which may include evidence of an expert.

In detail, Chapter 9 applies to electronic documents that can be submitted to court as evidence in civil and criminal law cases. Under Article 34 of the said Law, the content of a statement which is included in a document, that is regarded as admissible evidence, could be proven only by the presentation of the original document or, a copy of the original document provided that there is a sufficient justification for not presenting the original. This is a very useful legislative provision, in that it permits the admission of photo copies of all types in both criminal and civil proceedings whereas previously this was not possible except with the consent of the parties. Furthermore, an issue of fundamental importance is that of admissibility of evidence, and more specifically, of electronic evidence. Up to now, the Supreme Court has declared many times inadmissible evidence that had been obtained in breach of the provisions of the Cyprus Constitution. According to Clerides, "in the case of *Georghiades* (1982) the Supreme Court decided that tape recordings of a private conversation without the consent of the parties involved could not be admitted in evidence as obtained in violation of Articles 15 (private life) and 17 (respect of communication) of the Constitution. More recently in the case of *Police v. Doratis* (2006) the District Court following a trial within a trial (side trial) concluded that a CD containing copy of email exchanges between co-accused allegedly proving corruption could not be admitted in evidence".[928] Furthermore evidence obtained in breach of secondary legislation - such as Law 92(I)/96 - may be considered as inadmissible. "In the *Aeroporos* case computer printouts of the CYTA (Telecommunication Authority) recording the telephone numbers with whom the accused had been in touch at the material time, was held to be inadmissible under Article 3(2)(b) of the Law, which allows such evidence to be obtained only in cases not applicable. The evidence could not be admitted".[929]

Apart from the legislative framework governing electronic evidence, one needs to have a look at the Digital Evidence Forensic Laboratory (DEFL) that forms part of the Cyprus Police. The DEFL was established in 2009 and is responsible for the effective examination of electronic evidence. DEFL is staffed with specialised officers for the collection and forensic analysis of electronic devices. Their mission is the collection and forensic analysis of digital devices as well as the presentation of expert scientific evidence to the courts.

[927] This rule is also found in Article 14 of Law 119(I)/2000.
[928] Christos Clerides, The Law of Evidence – Lecture 9, https://www.clerideslegal.com/article/the-law-of-evidence-lecture-9
[929] Ibid.

14.4. Database Search

- **At international level**

The International Child Sexual Exploitation database, known as ICSE database, is used in the fight against sexual abuse of children. The ICSE database is the image and video comparison database of Interpol, into which CSE material is fed by security authorities worldwide. By analysing the digital, visual and audio content of photographs and videos, victim identification experts can retrieve clues, identify any overlap in cases and combine their efforts to locate the victims. Available through INTERPOL's secure global police communications system, I-24/7, certified users in member countries can access the database directly and in real time, providing immediate responses to queries related to child sexual exploitation investigations.[930] Cyprus is connected to the database along with various other Member States of the EU as well as third countries. Europol is also linked to the database.

The Child Protection System (CPS) is a UK-based software suite that law enforcement use to investigate crimes related to the sharing of child sexual abuse and exploitation images, available free of charge to all investigators. The CPS has the ability to monitor all known CSEM, whose names refer to sexually explicit material involving children and which are exchanged through direct Peer-2-Peer network file sharing programs. Peer-2-Peer is a network that allows two or more computers to share resources equally, i.e. any file that a user of the program downloads is automatically made available to other users upon their request. The use of such a network unites users from all over the world and is mainly used to copy and distribute music files, movies, software and others, which may be copyrighted without the consent of the copyright holder. The Cyprus Police has access to the online database of the CPS program, in which all the information of internet users who exchanged CSEM using the Peer-2-Peer network is stored. In detail, the Cyprus Police has access to specific details such as the IP address of the persons who exchange CSEM and the date and time, that are recorded and uploaded, on the said system. In order to gain access as to details regarding the user of the said IP address, they must obtain a court order.

The ICAC Child Online Protective Services (ICACCOPS) is an American police-based (FBI) intelligence gathering program that monitors in real-time Peer-2-Peer networks sharing and exchanging of child sexual abuse materials and indecent images of children, allowing for the identification of IP addresses which share and upload illegal material. The Cyprus Police has access to the ICACCOPS program.

The National Centre for Missing and Exploited Children (NCMEC) works closely with law enforcement officers in combating child exploitation. Law enforcement officers submit images and movies of children seized in CSE cases to NCMEC's Child Victim Identification Program (CVIP) for review.[931] The Cyprus Police has access to NCMEC via Europol.

- **At national level**

[930] Interpol network identifies 10,000 child sexual abuse victims http://virtualglobaltaskforce.com/interpol-network-identifies-10000-child-sexual-abuse-victims/

[931] Global alliance against child sexual abuse online https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/commitements/ga_commitment_-_united_states_en.pdf

The Cyprus Police is responsible for the management of a national image database, using the features of a software, titled GRIFFEYE,[932] used to examine the multimedia content of criminal investigations, respective categorization by type of abuse and the ages of the victims, in five categories - levels, and the preparation of an examination report to be used as documentary evidence in criminal investigations.

14.5. Use of Crawlers (Updated for Legal Report v2)

There is no specific legislation regarding search robots within the Cypriot legal framework. Some service providers operate, on a voluntary basis, a detection tool.

The Law on Certain Aspects of Information Society Services, in particular Electronic Commerce, and Related Matters (Law 156(I)/2004), that transposes Directive 2000/31/EC,[933] into Cypriot law governs the liability of service providers in general regarding illegal activity or information. More specifically according to Article 17(1) of Law 156(I)/2004, where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent, or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information, or (c) the provider stops using a link from the moment from the moment of becoming aware of the illegal content and of the fact that an infringement of the rights of third persons is being perpetrated through the page in question. According to Article 18 of the same Law, service providers have (1) no general obligation to monitor information being moved, nor a general obligation actively to seek facts or circumstances indicating illegal activity, when providing the services covered by sections 12, 13 and 14; and (2) an obligation to promptly inform the Competent Authority of alleged illegal activities undertaken or information provided by recipients of their service, and to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

More importantly, based on Article 11(3)(a) of Law 91(I)/14, internet service providers who provide services or internet access within the territory of the Republic are obliged, as soon as they become aware or as soon as they are informed by the service involved, such as the Cyprus Police or the Law Office of the Republic of Cyprus or the Ministry of Labour, Welfare and Social Insurance, about the existence of CSEM on any website, to take the appropriate measures to terminate their internet users' access on the said website. No court order is needed for such a termination to take place, on behalf of the internet service provider. Furthermore, according to Article 11(3)(b), violation of the abovementioned obligation constitutes a criminal offence, punishable by imprisonment of no more than three years or by a fine not exceeding one hundred and seventy thousand euros or both.

On a related note, CYTA, one of the biggest providers of integrated electronic communications services in Cyprus, explains, in its 2021 Annual Report, that it has implemented "Cleanfeed", a system that blocks access

[932] https://www.griffeye.com/

[933] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal, OJ L 178.

to websites with content that is illegal according to Cypriot law. The main sites to which access is restricted contain CSEM. With the introduction of this special system, all Cytanet customers have "clean Internet access".[934]

14.6. Cross-Border Cooperation and Cross-Border Exchange (Updated for Legal Report v2)

The Cyprus Police uses both European and international channels for cross-border cooperation and cross-border exchange of information.

At European level, it uses SIENA, the Secure Information Exchange Network Application. This platform enables the swift and user-friendly exchange of operational and strategic crime-related information among Europol's liaison officers, analysts and experts, Member States (including Cyprus) and third parties with which Europol has cooperation agreements. More specifically, the Large File Exchange (LFE) solution it offers, enables the secure exchange of files that exceed the size limit (50MB) of the Europol Secure Information Exchange Network Application when the need arises (for example sending an image of a hard drive or copy of a server).[935] Interestingly, according to Europol's Consolidated Annual Activity Report 2021, "in 2021, almost 718,000 large files were exchanged in LFE."[936] Furthermore, a tool of utmost importance for the Cyprus Police, is the European Investigation Order (EIO) in criminal matters as set out in Directive (EU) 2014/41,[937] constituting in practice, "a major step forward in judicial cooperation in criminal matters within the EU. [Undoubtedly it has]….become the main legal tool to gather trans-border evidence, replacing the traditional MLA conventions mainly used for this purpose so far".[938] In detail, the Cyprus Police regularly, requests the issue of an EIO by a judicial authority of the Republic of Cyprus, to have one or several specific investigative measure(s) carried out in another Member State, apart from Ireland and Denmark that are not bound by the said Directive. These investigative measures include, *inter alia,* a hearing by videoconference or other audiovisual transmission, covert investigations, interception of telecommunications, and other provisional measures.

At international level, Cyprus Police, through Europol, co-operates with the National Centre for Missing and Exploited Children (NCMEC) that works closely with law enforcement officers in combating child exploitation.

---

[934] CYTA, 2021 Annual Report, https://www.cyta.com.cy/mp/informational/cyta_htmlPages/media_center/annualreports/docs/AnReport_2021_en.pdf

[935] EUROPOL Intelligence: The Secure Information Exchange Network Application (SIENA), https://www.europol.europa.eu/annual_review/2015/intelligence.html

[936] EUROPOL's Consolidated Annual Activity Report 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202021.PDF

[937] The EIO is described in detail in sections 2.3.1, 2.3.2 and 8.4 above as well as the future instruments based on the final compromise text of the Draft eEvidence Package as agreed upon in January 2023.

[938] Jorge A. Espina Ramos, The European Investigation Order and Its Relationship with Other Judicial Cooperation Instruments Establishing Rules on the Scope and Possibilities of Application in EUcrim, Focus: Evidence Gathering – Current Legal Issues 1 (2009) pp.53-60.

Law enforcement officers submit images and movies of children seized in these cases to NCMEC's Child Victim Identification Program (CVIP) for review. Furthermore, Cyprus became a member of the International Police Organization (INTERPOL) in 1962. The National Central Bureau (NCB) for Cyprus is "part of the European Union and International Police Cooperation Directorate (EU-IPCD), a Headquarters Unit created to handle domestic police enquiries requiring international outreach. The NCB links the Cyprus Police Force to its worldwide counterparts and plays a central role in preventing the country and surrounding region from serving international organized crime".[939] One of the main INTERPOL information categories is CSEM and other offences against children.

[939] https://www.interpol.int/en/Who-we-are/Member-countries/Europe/CYPRUS

15. Country Report on Portugal

This Country Report aims to outline the framework regulating the fight against CSEM in Portugal. This fight is carried out on preventive and repressive vectors by several specially dedicated and qualified players legitimized by proper legal instruments.

15.1. Victims' Rights

Victim´s rights related to CSEM are based primarily on existing material and procedural provisions to protect the rights of minors, in particular their rights to sexual freedom and self-determination. As a member of the EU, the United Nations and the Council of Europe, all Portuguese domestic legislation is based on and respects the parameters defined by European Union Law and Public International Law emanating from those international organizations.

Portugal transposed the Budapest Convention and the Framework Decision 2004/68/JHA / Directive 2011/93/UE mainly by Law 59/2007, Law 109/2009 and Law 103/2015, establishing in the Portuguese legal order the set of material provisions (types of crime, liability of legal persons, application of law in space, etc.); instrumental provisions (System for the criminal identification of convicts for the practice of crimes against sexual self-determination and sexual freedom of minors, as well as Measures to prevent professional contact with minors, etc.); and penal procedural and international cooperation provisions as set by the Budapest Convention, opting to include the material provisions in the Penal Code and the instrumental, procedural and international cooperation provisions in special legislation.

The conformity of the Portuguese legal order to the fundamental legislative instruments referred above is always carried out in the spirit of Resolution of the Assembly of the Republic no. 16/2003 (Approves, for ratification, the Optional Protocol to the Convention on Children's Rights on the Sale of Children, Prostitution Child and Child Pornography, adopted in New York in 25 May 2000); and the Assembly of the Republic Resolution No. 75/2012 (Approves the Council of Europe Convention for the Protection of Children Against Sexual Exploitation and Abuse Rights, signed in Lanzarote on October 25, 2007).

Finally, Portugal takes into account the EU strategy for a more effective fight against child sexual abuse.

Still in the specific scope of the rights of freedom and sexual self-determination of minors, the signing of a Protocol between the Portuguese Safer Internet Centre and the LEA responsible for CSEM investigation is of fundamental importance.

Within the scope and in compliance with the provision of Directive 2011/93/EU, several entities constituted in consortium have proceeded to the signing of the INEA / CEF / ICTA2018 / 1633911 Agreement with the Innovation and Networks Executive Agency (INEA), which on its ARTICLE I.1 - SCOPE AND OBJECTIVES OF THE ACTION states:

> *The maintenance of a national platform to run a more secure range of Internet services, namely:*
>
> *i. An Awareness Service for the general public (Centro Internet Segura), based on digital resource repositories, of which specific toolkits and awareness services are adapted and implemented, in cooperation with third parties, such as schools, industry, other partners network, government agencies, associations and NGOs.*
>
> *As this service targets such a large population that covers very different and specific target groups,*

Centro Internet Segura has a coordination service to cover the school and educational community, which includes students (children and adolescents), teachers, parents and other professionals within the school curriculum. This coordination service is called SeguraNet, a brand that has been built since 2004.

ii. The Helpline service provided through telephone and online services, for the entire population, particularly aimed at children and parents to report and deal with harmful contact (for example grooming, online abuse), offensive conduct (for example, cyberbullying, hate speech, sexting) and unwanted or harmful content.

Beneficiaries will continue to develop their generic service delivery functions and will closely coordinate their activities with the main service platform and with the INSAFE and INHOPE networks.

iii. The Hotline Service to receive and manage reports and data on child sexual abuse content online and to cooperate with other stakeholders, such as the Police, hosts, dedicated entities, hotline network and Internet service providers and central EU service platform.

In 2019, the Helpline and Hotline lines were merged into a single line - Linha Alerta - competent under the terms of the Protocol signed with the PJ for accessing reports of illegal content, respective analysis and reporting to the authorities.

In the fields of NGOs is also worth mentioning the signing of a protocol with the Child Support Institute, manager of the SOS Child Line - 116 111. SOS Child Line is a free, anonymous and confidential service that supports children, young people, families, professionals and the community. The service aims to support the child, especially the child at risk, sexually abused and / or abused, missing, disintegrated from school, with conflicts with parents, who feels rejected or has suicidal ideation, seeking to find solutions for these situations.

With regard to Victims' Rights on penal procedures, Law 130/2015 proceeded to the twenty-third amendment to the Code of Criminal Procedure and approved the Statute of the Victim, transposing Directive 2012/29 / EU of the European Parliament and of the Council, of 25 October 2012 laying down rules on the rights, support and protection of victims of crime and replacing Council Framework Decision 2001/220 / JHA of 15 March 2001.

In a chapter especially dedicated to especially vulnerable victims, the following rights are granted to be enshrined in provisions in the most varied legislative instruments:

Article 22 – Rights of child victims

1 - All child victims have the right to be heard in the criminal proceedings, and for this purpose their age and maturity must be taken into account.

2 - In the event that there is no conflict of interest, the child may be accompanied by his parents, the legal representative or by those who have de facto custody during the deposition.

3-It is mandatory the appointment of a patron to the child when the interests of the child and that of his parents, legal representative or of those who have custody in fact are conflicting and even when the child with the appropriate maturity asks him to the court.

4 - The appointment of the patron is carried out under the terms of the law on legal aid.

5 - Information that could lead to the identification of a child victim should not be released to the

public, under penalty of its agents incurring the crime of disobedience.

6 - If the victim's age is uncertain and there are reasons to believe that it is a child, it is assumed, for the purposes of applying the regime provided for here, that the victim is a child.

Article 23 – Use of video or teleconferencing

1 - The testimonies and statements of the particularly vulnerable victims, when they imply the presence of the accused, are provided through videoconference or teleconference, as determined by the Public Prosecutor, unofficially or at the request of the victim, during the investigation phase, and by determination of the court, unofficially or at the request of the Public Prosecutor or the victim, during the phases of investigation or judgment, if this proves necessary to guarantee the provision of statements or testimony without constraints.

2 - The victim is accompanied, in the provision of statements or testimony, by a technician specially qualified to accompany him previously designated by the Public Prosecutor or the court.

Article 24 - Declarations for future memory

1 - The judge, at the request of the particularly vulnerable victim or the Public Prosecutor, may proceed with the earing of the victim during the course of the investigation, so that the testimony can, if necessary, be taken into account in the judgment, under the terms and for the purposes provided for in article 271 of the Code of Criminal Procedure.

2 - The Public Prosecutor's Office, the accused, the defender and the lawyers constituted in the process are notified of the time and place of the deposition so that they can be present, with the presence of the Public Prosecutor and the defender being mandatory.

3 - Statements are taken in an informal and reserved environment, with a view to guaranteeing, in particular, the spontaneity and sincerity of the responses.

4 - The making of declarations is carried out, as a rule, through audio or audio visual recording, and other means, namely stenographic or steno typical means, or any other technical means suitable to ensure the full reproduction of those, or documentation through self, only may be used when those primarily means are not available, what should be included in the record.

5 - The interrogation is made by the judge, and the Public Prosecutor's Office, the appointed lawyers and the defender can, in this order, ask additional questions, and the victim must be assisted during the procedural act by a technician specially qualified to accompany him and previously appointed by the court.

6 - In the cases provided for in this article, testimony should only be given at the hearing if this is indispensable for the discovery of the truth and does not jeopardize the physical or psychological health of the person who is required to provide it.

Article 25 – Access to reception facilities

Especially vulnerable victims may, if considered necessary in the context of individual assessment, be temporarily housed in state-supported care facilities.

Article 26 – Medical and medication assistance

1 - Especially vulnerable victims can be assisted by the health services integrated into the National Health Service located in the area of the reception structure where they are inserted, as an alternative to the health services of their residence.

2 - Particularly vulnerable victims are exempt from the payment of moderating fees within the scope of the National Health Service, under the terms to be regulated by order of the Government member responsible for the health area.

Article 27 – Social Communication

1 - The media, whenever they report situations related to the practice of crimes, when the victims are children or young people or other especially vulnerable people, cannot identify or transmit elements, sounds or images that allow their identification, under penalty of their agents to commit the crime of disobedience.

15.2. Data Protection

In terms of data protection, the Portuguese legislator has transposed Regulation 2016/679 and Directive 2016/680 of the European Parliament and of the Council, through Laws 58/2019 and 59/2019 respectively.

Regarding Directive 2016/680 and its relationship with Directive 2011/93, the provision in Recital 97 of Directive 2016/680 is worth noting: "(97) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93 / EU of the European Parliament and of the Council…".

Law 59/2019 establishes rules on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating or prosecuting criminal offenses or executing criminal sanctions, including safeguarding and preventing threats to public security, transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 into national law (Law 59/2017 Article 1).

This Law does not apply to the processing of personal data related to national security (Law 59/2017 Article 2).

According to Article 4 of Law 59/2017, personal data must be:

Subject to lawful and fair treatment;

Collected for specific, explicit and legitimate purposes, and cannot be treated in a manner incompatible with those purposes;

Adequate, relevant and limited to the minimum necessary for the pursuit of the purposes for which they are treated;

Accurate and updated whenever necessary and all reasonable measures must be taken so that the inaccurate data is erased or rectified without delay;

Kept in such a way as to allow the identification of the data subjects only for the period necessary for the purposes for which they are processed;

Treated in a way that guarantees their safety, including protection against their unauthorized or unlawful treatment and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

The LEA´s databases are regulated by law, being the one related to the PJ dated from 1999 and subject to legal regulation by Decree Law 352/99. The respective standards were already complied with the normative and legal regime established by Directive 95/46/EC, and are currently interpreted in the light of the legislation transposing Directive 2016/680.

Under the terms of Articles 1 and 2 of Decree Law 352/99, the existing computer files in the Judiciary Police are intended to organize and keep updated the information necessary for the exercise of functions, as well as providing the corresponding statistical elements; the collection of personal data for automated processing should be limited to what is strictly necessary to prevent a specific danger or to suppress specific criminal offenses. The different categories of data collected should, as far as possible, be differentiated according to the degree of accuracy or reliability, and factual data should be distinguished from those that involve an assessment of them.

15.3. Electronic Evidence

Criminal investigation increasingly needs access to and analysis of digital data. The widespread use of communication and information technologies has led to the introduction of new types of criminal offences in order to safeguard the confidentiality, integrity and availability of digital data. At the same time, this has created a distinct need of the judicial system for adequate tools enabling the investigation of these new crimes which are perpetrated with the help of such technologies.

In this matter, the Portuguese legal order is fundamentally governed by the legislation resulting from the transposition of the Budapest Convention through Law 109/2009.

Law 109/2009 establishes the material and procedural criminal provisions, as well as the provisions relating to international cooperation in criminal matters, relating to the field of cybercrime and the collection of evidence in electronic form, transposing Framework Decision No. 2005/222 to the internal legal order / JHA, of the Council, of 24 February, on attacks against information systems, and adapting domestic law to the Council of Europe Convention on Cybercrime (Law 109/2009 Article 1).

Pursuant to Article 11 of Law 109/2009, the procedural provisions relating to access, obtaining and use of data and electronic evidence in criminal proceedings apply to crimes:

- provided for in the Law 109/2009;
- committed by means of a computer system; or
- for which it is necessary to collect evidence in electronic form.

Contrary to the logic of legal construction underlying the Budapest Convention, crimes related to online sexual abuse are not included in Law 109/2009 since the Portuguese legislator opted to include such crimes in the chapter of the Penal Code dealing with crimes against freedom and sexual self-determination.

Following the logic of the criminal procedural system also in this area of electronic evidence, it is established

a general principle of the possibility of urgent and precautionary action by the LEA's, reserving to the magistrates the validation of such precautionary powers and the operationalization of investigative measures that contend with the people's rights and guarantees.

Thus, LEA´s are allowed to:

- request the expeditious preservation of electronic data with the authorization of the competent judicial authority or when there is an urgency or danger in the delay, in which case the LEA shall immediately inform the judicial authority of the fact and transmit a report provided for in Article 253 of the Code of Procedure Penal (Law 109/2009 Article 12);
- seize electronic data, without prior authorization from the judicial authority, in the course of computer search legitimately ordered and carried out under the terms of the previous article, as well as when there is urgency or danger in the delay, being apprehensions made by a criminal police body always subject to validation by the judicial authority, within a maximum period of 72 hours (Law 109/2009 Article 16).

It should be noted that Portugal maintains in force traffic data retention legislation for the purposes of criminal investigation – Law 32/2008, providing for the obligation of traffic data retention by telecommunications operators for a period of one year in the case of serious crimes. “Serious crimes”: crimes of terrorism, violent crime, highly organized crime, kidnapping, kidnapping and hostage-taking, crimes against cultural identity and personal integrity, against state security, counterfeiting of currency or securities equivalent to currency and crimes covered by convention on the safety of air or maritime navigation.

Article 1 of the Penal Procedure Code defines 'Violent crime' as a conduct that is intentionally directed against life, physical integrity, personal freedom, sexual freedom and self-determination or public authority and is punishable by a maximum prison sentence of 5 years or more – being the case of the most serious forms of online child abuse like production and transmission of illegal files (Article 176 of the Penal Code).

As Portuguese telecommunications operators are required by law to retain electronic traffic data for a period of six months for the purposes of commercial billing, such data may also be requested by a judge for the purposes of criminal investigation (Article 189 of the Penal Procedure Code; Article 11 of Law 109/2009)

Law 32/2008 is currently under consideration by the Portuguese Constitutional Court.

The conditions for accessing retained traffic data or for intercepting traffic data and content data are generally identical (Law 32/2008 Article 9; Penal Procedure Code Articles 187, 188, 189; Law 109/2009 Article 18):

The transmission of traffic data can only be authorized, by reasoned order from the investigating judge, if there are reasons to believe that diligence is indispensable for the discovery of the truth or that the evidence would be otherwise, impossible or very difficult to obtain in the context of the investigation, detection and prosecution of serious crimes.

The authorization provided for in the preceding paragraph may only be requested by the Public Prosecution Officer or by the competent criminal police authority.

The transmission of data must relate to:

- *The suspect or defendant;*
- *The person who acts as an intermediary, for whom there are reasonable grounds for*

believing that he receives or transmits messages intended for or coming from a suspect or defendant; or

- *The victim of a crime, with his or her consent, actual or presumed.*

The judicial decision to transmit the data must respect the principles of adequacy, necessity and proportionality, namely with regard to the definition of the categories of data to be transmitted and the competent authorities with access to the data and the protection of professional secrecy, under the terms legally provided.

The provisions of the preceding paragraphs are without prejudice to obtaining data on cell location necessary to rule out danger to life or offense to serious physical integrity, under the terms of article 252-A of the Criminal Procedure Code.

The collection of information by technical means is, as a rule, achieved from open or closed sources.

Open sources are those that are beyond the information accessible by free research in Information Technologies Processing and Communication, even if assisted by crawler programs, search engines or harvesters.

The privacy of communications and conversations between those present, in addition to their image, are examples of closed sources.

"Remote forensics" means a police technique, which is intrusively directed at a computer system, placing it without the knowledge or authorization of the one or more of its users, in the availability of third parties. These may:

- understand and record what is written on the normal or virtual keyboard;
- view what the camera embedded in that system can transmit;
- listen to what the built-in microphone can transmit;
- access the file system;
- view what the user performs on that system.

In the case described, it would be a total "remote forensics". This technology can also be of partial application, that is, only one or more of the five services indicated simultaneously.

In this way, what is referred to in a unitary way as "remote forensics", constitutes, in fact, a mix of interception of communications, of obtaining voice and image, as well as of access and remote search of files in a given computer system.

In Portugal "remote forensics" refers to a level of intrusion in private life only obtainable with legal authorization from the Investigating Judge.

The operationalization of this type of information collection is been conducted with reference to the regulatory regime for covert actions established by Law 101/2001.

As set on Law 101/20021 Article 3 these covert actions must be suitable for the purposes of criminal prevention and repression identified in concrete, namely the discovery of evidential material, and proportional to both those purposes and the seriousness of the crime under investigation. The deployment of the covert action within the scope of the investigation depends on prior authorization from the competent public

prosecutor, and must be communicated to the investigating judge and considered validated if no refusal order is issued within the next seventy-two hours.

If the covert action takes place within the scope of criminal prevention, the criminal investigating judge is competent for authorization, following a proposal by the Public Prosecutor.

Being a serious form of intrusion and embarrassment of rights, it can only be triggered with reference to defined crime catalogues:

Law 101/2001 Article 2

Voluntary homicide, as long as the agent is not known;

Against freedom and against sexual self-determination to which, in the abstract, a sentence of more than 5 years in prison corresponds, provided that the agent is not known, or whenever offenders under the age of 16 or other incapable persons are expressly mentioned;

Regarding the trafficking and addiction of stolen or stolen vehicles;

Slavery, kidnapping and kidnapping or taking hostages;

Trafficking in persons;

Terrorist organizations, terrorism, international terrorism and terrorist financing;

Capture or attack on the security of transport by air, water, railroad or highway to which, in the abstract, a sentence equal to or greater than 8 years in prison corresponds;

Executed with bombs, grenades, explosive materials or devices, firearms and trapped objects, nuclear, chemical or radioactive weapons;

Theft from credit institutions, public finance offices and post offices;

Criminal associations;

Relating to trafficking in narcotic drugs and psychotropic substances;

Money laundering, other goods or products;

Corruption, embezzlement and economic participation in business and influence peddling;

Fraud in obtaining or diverting a subsidy or subsidy;

Economic-financial offenses committed in an organized manner or using computer technology;

Economic and financial offenses with an international or transnational dimension;

Counterfeiting of currency, credit titles, sealed values, stamps and other similar values or the respective transfer;

Relating to the securities market.

Law 109/2009 Article 19

Covert actions provided for in Law no. 101/2001, of 25 August, under the terms therein, is permissible in the course of an investigation concerning the following crimes:

Those provided for in this law;

Those committed by means of a computer system, when, in the abstract, the maximum sentence of

imprisonment is greater than 5 years or, even if the penalty is lower, and being intentional, the crimes against freedom and sexual self-determination in the cases in which the offended ones are minors or incapacitated, the qualified fraud, the computer and communications fraud, racial, religious or sexual discrimination, economic and financial offenses, as well as the crimes enshrined in title iv of the Code of Copyright and Copyright. Related Rights.

If it is necessary to use computer means and devices, the applicable rules for the interception of communications are observed.

15.4. Database Search

At international level, the so-called ICSE database (International Child Sexual Exploitation database) is used in the fight against sexual abuse of children. The ICSE database is an image comparison database of Interpol, into which CSEM is fed by security authorities worldwide. Europol is also linked to the database.

Polícia Judiciária is responsible for accessing ICSE data base and the management of a national image database, using the features of the software used to examine the multimedia content of criminal investigations, respective categorization by type of abuse and the ages of the victims and preparation of an examination report to be used as documentary evidence in criminal investigations.

Since March 2020 PJ has been accredited with an account for access to the web platform of the National Centre for Missing and Exploited Children (NCMEC), which is operated via Homeland Security.

Access to reports produced by Canada's National Child Exploitation Crime Centre (NCECC) is secured via Europol.

The National Europol Office, within the structure of the PJ, ensures the accreditation of access to Europol's SIENA and LFE secure communication systems.

The Interpol National Office, which is also part of the PJ structure, equally guarantees access to Interpol's secure communication systems and the respective ICSdb.

LEA´s in Portugal frequently make use of cooperation operated via Liaison Officers, especially with the Portuguese Speaking Countries, highlighting in the area of Online Sexual Abuses the participation in Red Elipsia within the scope of EL PAcCTO (Europe Latin America Assistance Program for Combating Transnational Organized Crime).

15.5. Use of Crawlers

There is no specific legislation regarding crawler other than that resulting from the protection of personal data.

16. Country Report on Germany

This Country Report aims to outline the legal framework regulating the fight of Law Enforcement Agencies (LEAs) against CSEM in Germany. A special focus is given to the use of tools and devices benefiting from the capabilities of machine learning and/or artificial intelligence (AI). The use of AI tools by LEAs has to navigate the paradox that these very tools intended for improving public security can themselves become a source for public insecurity and even endanger fundamental freedoms. Therefore, the use of AI tools requires legal boundaries.

16.1. Victims' Rights

In Germany, the development of criminal procedures was driven for a long time by the effort of balancing appropriately the procedural interplay between the court, the prosecution and the accused. It was not until the 1980s that victims of crimes, especially of violent crimes have gained attention. This change was necessary because victims are not merely an object or proof for finding the accused guilty in criminal procedure. Rather, victims have legitimate interests to satisfaction of their own. Far from irrational vengeance, victims legitimately deserve official confirmation that the accused has done them wrong and caused them pain and suffering. The needs of victims go beyond criminal procedure and statutory rights. Victims are not only entitled to have justice, their dignity and their integrity restored, but also to governmental protection against further damages as well as governmental support in overcoming the trauma suffered.

Despite all efforts of crime prevention, anyone can fall victim to a crime.

The protection and support for victims is a societal task demanding a holistic approach. This approach only starts by granting victims legal claims to information, support and compensation. Ultimately, police, courts, schools and other institutions have to join hands to meet the legitimate interests of victims.

This section presents an overview of the legal rights and claims available to victims of CSE.

16.1.1. Criminal Procedure Rights

The German Criminal Procedure Code ("Strafprozessordnung, StPO") recognizes victims officially as party of criminal proceedings in order to keep them sufficiently informed about the proceedings. Section 406d StPO grants victims in general and also CSE victims the right to be informed about:

- the discontinuation and outcome of court proceedings in as much as it is relevant for the victim, section 406d(1) StPO;
- any order prohibiting the convicted person to contact or associate with the victim, section 406d(2)(No. 1) StPO;
- whether any measures involving deprivation of liberty are ordered or terminated against the accused or the convicted person or whether any relaxation or leave from prison are granted for the first time. While victims, in general, have to demonstrate the prevalence of their legitimate interest in these measures, victims of sexual abuse are exempted from this, section 406d(2)(No. 2) StPO.

Further, victims have the right to access records and pieces of evidence, section 406e StPO. Because of the strains they are facing, victims of CSE have the right to be represented by a lawyer as accessory prosecutor free of charge during the entire proceedings against the accused person, sections 397a(1) and 406g(3) StPO.

The tasks of such a victim's lawyer include pressing criminal charges, applying for measures of protection against violence, for access to prosecution files and court records, accompanying the victim to witness hearings and applying for witness protection measures. As accessory prosecutor, the victim has additional procedural rights including:

- the right to be present during court the entire proceedings including before the victim's witness hearing, section 397(1) StPO
- the right to refuse a judge or an expert witness on the basis of bias, section 397(1) StPO in connection with sections 24, 31, 74 StPO
- the right to questioning the accused, witnesses and expert witnesses, section 397(1) StPO in connection with section 240(2) StPO
- the right to object to questions, section 397(1) StPO in connection with sections 242 StPO
- the right to apply for proof, section 397(1) StPO in connection with sections 244(3)-(6) StPO, and the right to give statements after gathering of evidence, section 397(1) StPO in connection with sections 257(2) StPO
- the right to final statements, section 397(1) StPO in connection with sections 258(1) and (2) StPO
- the right to appeal, sections 400 and 401 StPO

16.1.2. Witness Protection

Victims of a crime, especially of a CSE are often the only witnesses of what happened. Therefore, witness statements of victims are crucial for criminal proceedings. Because victims of CSE have to re-live traumatising events in the course of their witness statement, there are several measures in place for their protection:

While section 68a StPO restricts the range of questions to the absolutely necessary, sections 171b and 172 Courts Constitution Act ("Gerichtsverfassungsgesetz – GVG") provide the option to exclude the public from the criminal proceedings for the protection of the victim. In addition, sections 168c and 247 StPO allow denying the accused person to be present at the victim's witness hearing, when the victim is deemed unlikely to say the whole truth in the presence of the accused person. In the interest of reducing the psychological distress for victims as much as possible, the witness hearing can be recorded once and then replayed at later stages of the criminal proceedings, sections 58a, 247a, 255a StPO. Alternatively and especially for vulnerable victims like children, the witness hearing can be arranged to take place audio-visually by locating the victim somewhere else than in the court room with all participants of the proceeding, section 247a StPO.

16.1.3. Compensation and Assistance for Victims of Violent Crimes

Anyone who suffers damage to his/her health as a result of a violent crime committed against himself/herself or against a relative is entitled to compensation under the Crime Victims' Compensation Act (CVC Act).[940]

[940] Crime Victims Compensation Act ("Opferentschädigungsgesetz – OEG") as promulgated on 7 January 1985 (Federal Law Gazette I p. 1), last amended by Article 2a of the Act of 15 April 2020 (Federal Law Gazette I p. 811).

Under the CVC Act, a violent crime is an intentional, unlawful physical assault against a person. Sexual offences and sexual assaults against minors are also regarded as violent crimes. The aim is to compensate for the health and economic consequences caused by such acts of violence.

Not only victims, but also people who were indirectly affected by the crime as well as surviving dependents are entitled to compensation via the Crime Victims Compensation Act.

- *Victims:* A person who has suffered damage to his/her health on account of an intentional, unlawful physical assault or as a result of lawfully defending himself/herself against such an assault. This also includes persons who suffer an impairment of health due to shock by witnessing said crime.
- *Indirectly affected:* Victims' dependents, who weren't present at the scene of the crime, but have a close personal relationship or are related to the victim.
- *Surviving dependents:* If the victim is deceased, certain close relatives have a claim to surviving dependents pensions, regardless of damage to their own health.

Anyone who becomes victim of an intentional act of violence within the territory of the Federal Republic of Germany and suffers health damage as a result is entitled to file for compensation. The same goes for the surviving dependents of anyone who died as a result of a violent act. Under certain conditions, foreign nationals are also entitled to victims' compensation.

In the case of violent crimes committed in Germany, victims are entitled to compensation for all resulting physical and mental health impairments. Compensation is also paid for economic damage resulting from such damage to health.

The extent and amount of the benefits available are set out in the Federal War Victims Compensation Act. They include in particular:

- Curative and medical treatment, long-term care,
- Aids (e.g. prostheses, dental prostheses, wheelchairs),
- Compensation paid to victims and surviving dependants,
- A funeral allowance,
- Other welfare benefits in the event of economic need (e.g. long-term care benefit, subsistence allowance).

16.2. Data Protection

Regarding crime investigations by LEAs, personal data is protected in accordance with a specific legal framework. According to Art. 2(2)(d) GDPR, the General Data Protection Regulation (GDPR) does not apply to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. These areas including criminal investigations by LEAs fall under the regulatory framework established in Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive). The Law Enforcement Directive has been transposed into German law in the sections 45 – 84 Federal Data Protection Act

("Bundesdatenschutzgesetz, BDSG"). However, these (general) provisions of the BDSG are subsidiary to specific special laws as stated in section 1(2) sentence 1 BDSG. Two such special data protection laws are the Federal Criminal Police Office Act ("Bundeskriminalamtgesetz, BKAG") and the German Criminal Procedure Code ("Strafprozessordnung, StPO").

16.2.1. General Principles for Processing Personal Data

The interplay between StPO and BDSG is regulated in section 500 StPO stating that sections 45 – 84 BDSG are applicable to law enforcement only if the StPO does not contain any more specific provisions. The general principles for processing personal data are regulated in section 47 BDSG. According to section 47 BDSG, personal data shall be:

1. processed lawfully and fairly;
2. collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
3. adequate, relevant and not excessive in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Further requirements are established in section 48 BDSG for processing special categories of personal data. According to section 46 No. 14 BDSG, the term "special categories of personal data" refers to (a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (b) genetic data; (c) biometric data for the purpose of uniquely identifying a natural person; (d) data concerning health; and (e) data concerning a natural person's sex life or sexual orientation. The processing of any of these "special categories of personal data" is allowed only where strictly necessary for the performance of the controller's tasks, section 48(1) BDSG. If special categories of personal data are processed, appropriate safeguards[941] for the legally protected interests of the data subject are to be implemented, section 48(2) BDSG.

[941] According to section 48(2) BDSG appropriate safeguards in this regard may be in particular (1) specific requirements for data security or data protection monitoring; (2) special time limits within which data must be reviewed for relevance and erasure; (3) measures to increase awareness of staff involved in processing operations; (4) restrictions on access to personal data within the controller; (5) separate processing of such data; (6) the pseudonymization of personal data; (7) the encryption of personal data; or (8) specific codes of conduct to ensure lawful processing in case of transfer or processing for other purposes.

16.2.2. Specific Regulations for Processing Personal Data

As specific regulations concerning criminal investigations by LEAs, section 161(3) StPO and section 479(2) StPO deserve special attention. Section 161(3) StPO provides that if a measure under this Act is only permissible on suspicion of certain criminal offences, the personal data obtained on the basis of a corresponding measure under other laws may, without the consent of the persons affected by the measure, be used for evidentiary purposes in criminal proceedings only for the purpose of clarifying such criminal offences for the clarification of which such a measure could have been ordered under this Act. Section 479(2) StPO explicitly refers to section 161(3) StPO regarding measures taken on suspicion of a certain offences. Furthermore, section 479(2) sentence 2 and (3) StPO stipulates that personal data may only be used for the following purposes without the consent of the person concerned:

1. for security purposes, insofar as they could be collected for this purpose by a corresponding measure under the laws applicable to the competent body,
2. to avert a danger to the life, limb or freedom of a person or to the security or existence of the Federation or of a Land or to significant assets, if the data in the individual case reveal concrete approaches to averting such a danger,
3. for the permissible transmission of information to the constitution protection authorities pursuant to section 18 of the Federal Constitution Protection Act, or
4. for information and file inspection for research purposes in accordance with section 476 StPO.

Data collected in the course of acoustic surveillance of living quarters (section 101c StPO), online searches (section 101b StPO) or collection of traffic data (section 101g StPO) may also be used in certain other dangerous situations according to section 479(3) StPO. These requirements for the use of the different types of data reveal that the answer to the question to what extent personal data may be used ultimately depends on an examination of the individual case.

16.3. Electronic Evidence

LEAs are permitted to investigate a case, if an offence is given or if danger is imminent. Evidence has to be seized or secured and especially in the field of electronic evidence it is important to secure evidence in such a way, that subsequent distortions are eliminated. All determinations and evidence securings are based on the relevant legislation of the respective authority. Common violations that can compromise criminal investigations or proceedings are:

- Violation of the obligation to notify (section 168c(5) StPO),
- Violation of the order conditions to perform telecommunications surveillance (section 100a StPO) or undercover investigation (section 110a StPO)
- Specific collections of evidence have to be mandated by the public prosecutor's office
- Sometimes the act of collecting evidence, that significantly violates the fundamental rights of a person, requires the affirmation of a judge
- Violation of the legal provision (considering also the police laws of every Federal State)

Definition: Electronic evidence means all information, stored or transmitted in a digital form, which is relevant

for a specific criminal investigation.

- **Procedure for obtaining electronic evidence**

Electronic evidence is obtained in particular through the search and seizure of media, on which or where digital data is stored, and through the collection of digital data (subscriber data, traffic data and content data) via the involvement of the service provider.

The Federal Criminal Police Office ("Bundeskriminalamt, BKA") is part of the 24/7 network for urgent matters and will contact also in urgent cases provider and/or prosecutor offices in charge. As each prosecution office has a 24/7 service, a prosecutor from the competent prosecutor´s office can always be reached.

The competent public prosecutor´s office is the one in whose area of competence the requested measure is to be carried out and German is the only language accepted.

- **Categories of Data**

The **subscriber data** includes data that the provider stores for the owner of an account in order to be able to properly process the contract, e.g. telephone number or mailbox identifier, name and address of the holder, date of birth, date of contract start and end, contract information and tariff characteristics.

Insofar as it is necessary to establish the facts or determine the whereabouts of an accused person, information on subscriber data may be requested from any person providing or collaborating in the provision of telecommunications services on a commercial basis.

The information may also be requested by reference to an Internet Protocol address assigned to a specific time.

No **threshold** exists in relation to the subscriber data and IP-addresses.

Traffic data includes inter alia phone number or other identifier of the calling and called connection or the respective terminal equipment, personal authorization identifiers, the card number for customer cards and the location identifier of the sender or recipient for mobile connections. Furthermore it includes inter alia the start and end of the connection according to the date and time, the amount of data transmitted, the protocol used, the format of the message, the network from which the message originates or to which it is sent, the telecommunication service used, and the endpoints of committed ones connections as well as their time and duration and other connection data required for the establishment and maintenance as well as for payroll accounting.

Threshold: Orders for the release of **traffic data** are subject to strict requirements. According to Section 100g StPO, they may only be released either

- if someone is suspected of a criminal offense "of considerable importance, even in individual cases" (such as e.g. murder, homicide, distribution, acquisition or possession of youth or child pornography, robbery, fraud, computer fraud etc.) or
- if he is suspected to have committed an offence by means of telecommunications.

Moreover, the collection of particularly sensitive traffic data must be necessary for the investigation of the facts of the case and the collection of the data must be proportionate to the importance of the matter.

Content data is any data stored in a digital format related to the content of a communication (text, voice, videos, images and sound other than subscriber or traffic data).

Threshold: Due to the intervention-intensive character, content data can only be obtained via telecommunication surveillance if

(i) certain facts give rise to the suspicion that a person has, either as an offender or participant, committed a specific serious crime of the kind referred to in Section 100a(2) StPO[942]

(ii) the offence is one of particular severity in the individual case as well and

(iii) other means of establishing the facts or determining the accused's whereabouts would be much more difficult or would offer no prospect of success.

- **Admissibility:**

Electronic evidence obtained by voluntary disclosure is admissible.

- **Data retention periods (including procedures for extensions)**

The German Telecommunication Act ("Telekommunikationsgesetz, TKG") provides for retention periods between 4 and 10 weeks:

- 4 weeks for location data of the participants of all mobile phone calls at the beginning of the call and location data at the beginning of mobile internet use, section 113b(1)No.2 TKG;
- 10 weeks for phone numbers, time and duration of all phone calls, sending and receiving times of all SMS messages, assigned IP addresses of all Internet users as well as time and duration of Internet use, section 113b(1)No.1 TKG.

However, the application of the data retention provisions in Germany is currently suspended as the German Federal Administrative Court ("Bundesverwaltungsgericht, BVerwG") decided in September[943] to transfer the final interpretation of the data protection Directive for electronic communication (Directive 2002/58/EG) to the Court of Justice of the European Union (CJEU). Until the final clarification of the CJEU, the data retention provisions in Germany remain suspended and data is only stored as long as this is necessary for billing purposes.[944] However, in the light of the CJEU's most recent decision concerning data retention[945], the CJEU seems to develop a line of case law which renders the German approach set out in section 113b TKG most unlikely not to be in breach of European law. For the time being therefore, the storage time differs from one provider to another.

[942] Section 100a(2)(g) StPO refers to the crime of distributing, acquiring or possessing youth or child pornography as stated in sections 184b und 184c German Criminal Code ("Strafgesetzbuch, StGB").
[943] BVerwG, decision of 25 September 2019 in case 6 C 13.18, available at: https://www.bverwg.de/250919B6C13.18.0.
[944] BNetzA, „Mitteilung zur Speicherverpflichtung nach § 113b TKG", 28 June 2017, available at: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html.
[945] CJEU, decision of 2 March 2021 in case C-746/18 – H.K. v. Prokuratuur, available at: https://curia.europa.eu/juris/document/document.jsf?docid=238381&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=7374266.

16.4. Database Search

At international level, the so-called ICSE database (International Child Sexual Exploitation database) is used in the fight against sexual abuse of children. The ICSE database is an image comparison database of Interpol, into which CSEM is fed by security authorities worldwide. Europol is also linked to the database.

As the central office the Federal Criminal Police Office ("Bundeskriminalamt, BKA") is responsible for data maintenance in Germany. The aim is – as with the national image comparison database – to be able to compare newly received abuse material with the database in order to be able to determine whether it can be assigned to a case that has already been solved or whether intensive investigative measures are required to solve the case of abuse.[946]

- **ICSE Database**

The ICSE database is essential for any BKA cases involving sexual abuse material. It provides real-time responses to queries, allowing users to establish whether they are dealing with new, known or maybe even identified material. This helps avoid duplicating efforts. The overall assessment shows that the systematic collection and comparison of material provides valuable clues for investigations. The material is stored in a database with relevant case data and additional information and is immediately available for queries posed by other member countries. The added value of the ICSE database has been growing constantly with the rising number of participating countries and active users.[947]

- **HashDB PS Database**

As the "Central Office for Combatting Sexual Offences Against Children and Adolescents"[948], the BKA also operates the (national) hash database Pornographic Writings (HashDB PS). The database is used in the BKA in a specially developed workflow for the automated pre-assessment of files relevant to criminal law. These are checked for hash value similarity or photo-DNA similarity and automatically evaluated. This makes it possible to efficiently process the tips received daily by the BKA regarding the possession and distribution of CSEM (quantity) and to achieve a high level (quality).[949]

The hash database for child pornographic writings (HashDB PS) is a collection of hash values of known child and youth sexual exploitation material which the BKA makes available to the federal states for matching

[946] Antwort der Bundesregierung v. 12.5.2020 auf die Kleine Anfrage diverser Abgeordneter und der Fraktion der FDP zu „Legal Tech bei Sicherheitsbehörden", Bundestag Drucksache Ds. 19/19105, Seite 7.
[947] De Maizière, „Interpol's International Child Sexual Exploitation Database", 4 November 2014, available at: https://www.bmi.bund.de/SharedDocs/reden/EN/2014/interpol.html.
[948] Zentralstelle für die Bekämpfung von Sexualdelikten zum Nachteil von Kindern und Jugendlichen, BKA: https://www.bka.de/DE/UnsereAufgaben/Aufgabenbereiche/Zentralstellen/Kinderpornografie/kinderpornografie_node.html.
[949] Bericht der Bundesregierung über die im Jahr 2017 ergriffenen Maßnahmen zum Zweck der Löschung von Telemedienangeboten mit kinderpornografischem Inhalt im Sinne des § 184b des Strafgesetzbuchs, September 2018, Seite 22; Antwort der Bundesregierung v. 12.5.2020 auf die Kleine Anfrage diverser Abgeordneter und der Fraktion der FDP zu „Legal Tech bei Sicherheitsbehörden", Bundestag Drucksache Ds. 19/19105, Seite 10.

purposes. If a data carrier is seized in the federal state, it can be compared with the collection and provides initial indications of the contents of the data carrier. This enables a faster and more efficient evaluation of the seized evidence.[950]

- **Image Database**

The BKA also uses an image database developed by an external company, in which image and video material on identified and unidentified victims and perpetrators of sexual abuse is centrally stored for the whole of Germany. The database is used to assign newly received data to already known series of sexual abuse of children in order to avoid duplication of work and re-victimisation.[951]

16.5. Use of Crawlers

The usage of search robots is not mentioned within the German legal framework.

Criminal Liability: Every crime necessitates a deliberate intention to commit the offence. That means, an individual acting within the capacities of a LEA will not be liable to prosecution, when monitoring and analysing CSEM (sections 184 et seq. of the German Criminal Code ("Strafgesetzbuch, StGB"). The collection and storage of CSEM for the purpose of the evaluation of evidences (sections 94 and 98 StPO) or the prosecution of a criminal offence (section 163 StPO) is not illegal in Germany.

Investigative Competences: According to section 163 StPO German authorities and officials in the police force shall investigate criminal offences and shall take all measures that may not be deferred, in order to prevent concealment of facts. This law ensures the exclusion of offences when authorities and officials in the police force are investigating, for example in the following fields:

- dissemination, procurement and possession of child pornography, section 184b StGB,
- dissemination, procurement and possession of youth pornography, section 184c StGB and
- organisation and attendance of presentations of child and youth pornography, section 184e StGB.

The investigative competences of LEAs are regulated in section 163 StPO. This provision also includes online investigations within sources accessible by the public like newsgroups, public chats or social networks. In addition, it is permitted to communicate in social networks with the use of a false identity. However, this will not apply in case of an infringement of telecommunications secrecy or a permanent participation at closed user groups with the use of a legend or by overcoming the access control (section 110a StPO).

Copyright Infringement: As competent authorities, LEAs may make copies of portraits or to have these reproduced for the purposes of the administration of justice and public security, section 45 of the German Copyright Act ("Urheberrechtsgesetz, UrhG").

[950] Bericht der Bundesregierung über die im Jahr 2017 ergriffenen Maßnahmen zum Zweck der Löschung von Telemedienangeboten mit kinderpornografischem Inhalt im Sinne des § 184b des Strafgesetzbuchs, September 2018, Seite 22; Antwort der Bundesregierung v. 12.5.2020 auf die Kleine Anfrage diverser Abgeordneter und der Fraktion der FDP zu „Legal Tech bei Sicherheitsbehörden", Bundestag Drucksache Ds. 19/19105, Seite 10.

[951] Antwort der Bundesregierung v. 12.5.2020 auf die Kleine Anfrage diverser Abgeordneter und der Fraktion der FDP zu „Legal Tech bei Sicherheitsbehörden", Bundestag Drucksache Ds. 19/19105, Seite 9.

Electronic Evidence: Concerning the proper procedures for obtaining electronic evidence (section 1.3 above), exceptions may be made. Inter alia, it may be possible to accept illegally obtained evidence by mandating investigations retrospectively. In addition, evidence which is discovered accidentally or coincidentally (dt.: “Zufallsfunde”) may be accepted in criminal proceeding, but has to be approved by the public prosecutor's office or by a judge. The “fruits of the poisonous tree doctrine” is not known and accepted in Germany.

Agent provocateur: The German legal framework for the use of an agent provocateur is very complex. If a person has committed a crime because he was encouraged to do so by an individual acting within the competences of a LEA, the responding Federal State has to conduct criminal proceedings. However, the act of encouraging an individual to commit a crime violates the basic principle of fair proceedings and will lead to a procedural impediment (section 26 StGB; Art. 6 Abs. 1 EGMR). In practice, individuals acting within the competences of a LEA as agent provocateur are not allowed to encourage a person to commit a serious crime. Exceptions may be made for light offences like joining a demonstration or showing illegal material in order to maintain the fictional legend.

17. Country Report on Lithuania

17.1. Victims' Rights

17.1.1. General Legal Framework

- **Implementation of EU Directive 2011/93/EU**

Lithuania has adhered to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 2012[952]. Legal requirements of The European Parliament and of the Council Directive 2911/93/EU[953] on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing the Council Framework Decision 2004/68/JHA were introduced in national law by amendments made to the Criminal Code[954], Criminal Procedure Code[955], also amendments to the Law on Operational Activities[956].

Amendments to the Code of Criminal Procedures (CCP) were introduced defining requirements on closed court hearings and video and audio recording requirements during investigation, when a child was identified as a victim. According to the Art. 186 (2, 3) of CCP, a juvenile witness or juvenile victim shall normally be interviewed during the pre-trial investigation in premises adapted for the examination of children. The interview should be organized only once. National case law highlights that interviewing only once should be the priority of all the courts and the main rule[957]. In exceptional cases where a pre-trial investigation requires a re-interviewing of a minor witness or a minor victim, they shall normally be questioned by the same person. A video and audio recording must be made of their interview. The juvenile witness and the victim are usually questioned by the pre-trial judge during the pre-trial investigation. A juvenile witness and a juvenile victim shall be summoned to a court hearing only in exceptional cases.

The representative of a juvenile witness or juvenile victim has the right to participate at the interrogation if it does not affect the juvenile. Taking into account a juvenile witness or juvenile victim social and psychological maturity a representative of the State Child Rights Protection Service or a psychologist must be invited to the interview if requested by the representative of a juvenile witness or juvenile victim or on the initiative of the pre-trial investigation officer, the prosecutor or the court (Art. 186 (5), Art. 280 (1) of CCP).

In order to protect the interviewed juvenile from adverse effects, the suspect (accused) or other participants in the proceedings (except a representative of the State Child Rights Protection Service or a psychologist) may not be allowed to participate in the same interrogation room. In such a case, an audio and video recording must be made, and the suspect and other participants in the proceedings must be given the opportunity to observe and hear the interrogation from another room and to ask the interrogated person questions through

[952] Law on the Ratification of The Council of Europe Convention for the Protection of Children From Sexual Exploitation and Sexual Abuse https://www.e-tar.lt/portal/lt/legalAct/TAR.78F8E311B33C

[953] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

[954] The Law amending articles 7, 8, 27, 60, 95, 97, 151, 1511, 153, 162, 307, 308, 309 of The Criminal code and amending supplement to the annex and articles 1001, 1002, 1521, 2511 https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/54910c10ae9c11e39054dc0fb3cb01ae

[955] The Law amendment articles 9, 154, 186, 280, 283 of the Criminal Procedure code and amending the annex to the code https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/b090aed0ae9c11e39054dc0fb3cb01ae

[956] The Law amending article 8 of The Criminal intelligence law https://www.e-tar.lt/portal/lt/legalAct/0a57b100b57f11e3ad2eed5a4e1b7108

[957] For example, The Supreme Court of the Republic of Lithuania case No. 2K-594/2012.

the pre-trial judge (Art. 186 (3, 4), Art. 280 (3) of CCP). The precise procedures are described in Recommendations of Prosecutor General of the Republic of Lithuania "For the Assessment of the Needs of Special Protection for the Victims[958]" adopted on 29 February 2016.

- **Implementation of EU Directive 2011/36/EU**

Legal requirements of The European Parliament and of the Council Directive 2011/36/EU[959] of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, were introduced in national law by amendments to The Law on Fundamentals of Protection of the Rights of the Child[960].

These amendments introduced the main measures for the protection of the rights of the child. Provisions that define the general measures stipulating that a child who has been the victim of a crime, violence or other ill-treatment must be provided with the necessary assistance to recover and be integrated into the social fabric of society. Significantly, the institutional framework to provide support for these victims has been defined.

The European Commission in 2019 initiated an infringement procedure against Lithuania (2019/2134)[961] regarding implementation of requirements of Article 3(5) and Article 9(b) and (g) Directive 2011/93/EU. To harmonize national law with this EU Directive's requirements, amendments to the Criminal Code (CC) were drafted in January of 2020[962]. For example, Art. 151^1 of CC was amended by enacting the criminal liability for engaging in sexual activities with a child, where abuse is made of a recognised position of trust, authority or influence over the child by any person not only parents or guardians as it was before. Also, the Art. 60 of CC was amended by enacting offence committed by a member of the child's family or a person cohabiting with the child as aggravating circumstances. There were no infringements identify related to CCP.

The European Commission in 2016 initiated an infringement procedure against Lithuania (2016/0109) regarding implementation of requirements, and regarding the European Parliament and of the Council Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA and the implementation of requirements of Directive 2011/36/EU, as well as regarding establishment of a legal and institutional framework for the victims of crime. To harmonize national law with these EU Directives' requirements amendments to the Law on Fundamentals of Protection of the Rights of the Child, as well as amendments to the Law on Social Services and new Law on Assistance to Victims of Criminal Activities were drafted in September of 2020[963]. The amendments to the Law on Fundamentals of Protection of the Rights of the Child were formal because all the provisions of this law were in a line with the requirements of Directive 2012/29/EU but the Directive was simply not mentioned among the implemented laws. Additionally, it enacted that the provisions of the Law on Social Services, the Law on Victims and the Law on Assistance to Victims of Criminal Activities also apply to the children.

[958] https://www.e-tar.lt/portal/lt/legalAct/86bc22f0dfa611e58a92afc65dd68e97
[959] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32011L0036
[960] The Law on Fundamentals of Protection of the Rights of the Child https://www.e-tar.lt/portal/lt/legalAct/TAR.C8205E261830/asr
[961] https://ec.europa.eu/commission/presscorner/detail/EN/INF_19_4251
[962] https://www.e-tar.lt/portal/lt/legalAct/1db95560429f11ea829bc2bea81c1194
[963] https://www.e-tar.lt/portal/lt/legalAct/6f64074006f611ebb74de75171d26d52

17.1.2. Specific Sexual Abuse Victims' Rights

To protect sexual abuse children rights, various remedies are defined in national laws. To categorise existing measures, one could protect victims' rights of the investigation process and court proceedings, including victims' rights to receive adequate social and psychological support, as well as measures granting victims the right to receive legal advice and compensation.

- ***Victims' rights during the investigation and Court hearing process***

To reduce negative psychological impact to the child in the investigation process and court hearings, the general requirement to interview victims no more than once during a pre-trial investigation is defined. The criminal process code allows for the making of audio (or video) records, of the interview, which could be presented to the court. In this case, the testimony given by the victim to the pre-trial judge must be read aloud in court. If a suspect or his lawyer is present at the examination of a witness or victim under the age of eighteen, the pre-trial judge must ensure that such witness or victim is not unduly influenced. (Articles 186, 280, 283 CCP) . Witnesses and victims under the age of eighteen are invited to a court hearing only in exceptional cases.

Article 9(3) CCP also states that cases may be heard in private in court, inter alia, for criminal acts on the freedom and inviolability of a person's sexual self-determination and cases in which persons under the age of eighteen are charged.

- ***Victims' rights to receive adequate social and psychological services***

The Law on Fundamentals of Protection of the Rights of the Child and the Law on Social Services of the Republic of Lithuania[964] defines cases when a child could be provided social and psychological or other needed support or services. The law requires institutions to respond to any reported violation of a child rights (including criminal offence) in 3 days. It should be added that the law defines that in every case, individual assessment should be made and adequate measures, including social, psychological treatment or other services have to be provided (Articles 35, 36). We emphasise too that in the past several years in general all measures were oriented to reduce domestic violence against the child. Even the law defines a requirement to assess each case individually, for participating organizations to provide support to sexual abuse victims.

- ***Victim rights to receive legal advice and compensation***

The law on state-guaranteed legal aid[965] defines that sexual abuse victims are eligible to legal aid in criminal proceedings by the decisions of a pre-trial investigation officer, prosecutor or the court.

The Law on Compensation for damage caused by violent crimes[966] defines the right of sexual abuse victims to receive compensation from the state.

L3CE interviewed NGO's related to child rights protection and other responsible authorities and identified the following issues and risks related to framework implementation:

[964] The Law on Social Services https://www.e-tar.lt/portal/lt/legalAct/TAR.91609F53E29E/asr
[965] The Law on state guaranteed legal aid https://www.e-tar.lt/portal/lt/legalAct/TAR.EAA93A47BAA1/asr
[966] The Law on Compensation for Damage Caused by Violent Crimes https://www.e-tar.lt/portal/lt/legalAct/TAR.0258F89BCE57/asr

- Poor competences and knowledge to identify cases when a child is offended online. The law defines clear responsibilities and an institutional framework to report indicated sexual abuse cases against the child, but the gap of knowledge to indicate such cases related with child activities online, delays adequate response.
- Competences and knowledge of experts varies depending on the organization or geographical distribution (regions). The lack of knowledge in sexual abuse victim's treatment raises the risk that adequate support to a child would be provided.

Inadequate or non-consistent institutional system to provide protection for victims of criminal offence. National regulation clearly defines a general institutional framework and possible measures to be provided ensuring protection of child rights. But in criminal offence cases, the child and (or) his family needs to go all the way to receive adequate protection or state provided services. Usually different NGO's which have a common view of the situation does help and leads the victims in the criminal offence cases (offence reporting; providing primary legal advice and help to receive state paid legal services; initiation of social and psychological services, etc.). New policy initiatives drafted on the September of 2020 (The Law on Fundamentals of Protection of the Rights of the Child, amendments to The Law on social services and New law On Assistance to victims of criminal activities) should change this situation in essence. The new law defines one focal point (Police; or New organization) which has to lead and manage state services provision for the victims.

17.2. Data Protection

The processing of personal data within the Police of Lithuania is governed by internal rules on the processing of personal data in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR), the Law of the Republic of Lithuania on Legal Protection of Personal Data, the Law of the Republic of Lithuania on Legal Protection of Personal Data, Processed for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences, or the Execution of Criminal Penalties, or National Security, or Defence and the Law of the Republic of Lithuania on Police[967].

The collection of electronic evidence (personal data) for the purpose of crime investigation is regulated by CCP. The main regulatory issue is defining different personal data protection levels depending on whether context of communication or metadata is collected as well. Also, different requirements apply for collecting of prospective, retrospective and real time personal data transmitted by cyber space. For example, electronic surveillance of prospective and real time content of electronic communication is regulated by Art. 154 of CCP. This type of personal data could be collected only upon a justified court order. On the other hand, metadata can be collected either in accordance Art. 155 of CCP upon court decision (with no justification) or in accordance Art. 97 of CCP with no court order at all. To point out, Art 22 of the Constitution of the Republic of Lithuania states that „information concerning the private life of a person may be collected only upon a justified court decision and only according to the law". Consequently, the constitutional compatibility of above mentioned regulation allowing collection of metadata (personal data) as well as retrospective content of communication without justified court order should be questioned and considered illegal.

Furthermore, there is no special regulation of law enforcement hacking while it is used to obtain electronic evidence in Lithuania. According to the Attorney General Recommendations on the Application of the Provisions of the Law on Criminal Intelligence, the Code of Criminal Procedure and the Use of Criminal

[967] https://policija.lrv.lt/en/data-protection

Intelligence Information in Criminal Proceedings 17 law enforcement hacking is equivalent to the actions of a secret agent and therefore is regulated by the same in accordance to the Art. 158 of CCP. Consequently, there is no special provisions in Art. 158 of CCP concerning special requirements for the lawful restriction of the right to privacy laid out in the case law of European Court of Human Rights[968]. Additionally, the study ordered by European Parliament "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices"[18] concludes that law enforcement hacking restricts the right to privacy the most. Therefore, according to above mentioned study, ex ante and ex post control mechanisms of law enforcement hacking has to be clearly establish in the laws, regulating it. However, current regulation of law enforcement hacking in Lithuania does not meet this requirement since there is no specific regulation.

17.3. Electronic Evidence

17.3.1. Overview on Regulation, Collection and Recording

According to Article 20(1) Code of Criminal Procedure (hereinafter CCP), "Electronic Evidence in criminal proceedings is obtained in accordance with the procedure established by the national law". The national CCP does not distinguish between separate groups of electronic and / or digital evidence, therefore the electronic evidence obtained using AI and ML techniques falls under the same Article 20, of the CCP.

Referring to the CCP, electronic evidence obtained during the criminal proceedings must be collected in a way that meets certain criteria. It must be:

- Admissible
- Authentic
- Complete
- Reliable
- Credible
- Proportional

In addition, the requirement determining the relevance of electronic evidence during pre-trial investigation must be in line with the General Principles for Electronic Evidence set out in ISO 2737, which states that evidence must be:

- Relevant: device must be useful for the investigation of a crime.
- Faithful: reliability and persuasiveness of the evidence provided.
- Sufficient: The number of devices added to the study must be sufficient provable (significant)

Five basic principles on the handling of electronic evidence are followed by pre-trial investigation agencies in Lithuania:

- Principle 1 – Data Integrity. No action taken that would alter the digital device or media which

[968] egz. *Klass and others v. Germany*, *Malone v. UK*, *Huvig v. France*, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, *Dragojević v. Croatia* , *Rotaru v. Romania* and etc.

may subsequently be used in the court as credible evidence.

- Principle 2 – Audit Trail. The process of taking, seizure, access, processing, transport and storage of evidence must be recorded. An independent third party should be able to examine those processes and achieve the same result.
- Principle 3 – Specialist Support. During the course of planned operations, it is mandatory to call a specialist and ensure their presence during the search and seizure. It must be ensured by the person in charge of the case, especially if the digital device can be expected or if equipment may be critical to the case.
- Principle 4 – Appropriate Training. Every person handling electronic evidence must have appropriate training to perform their duties.
- Principle 5 – Legality. The process for taking and processing digital evidence must be in line with existing legislation.

Lithuanian police continually invest in digital investigation capabilities[969]. Modern technologies like advanced automation in digital forensic investigation combined with ML used in digital forensics helps to shorten e-evidence collection, validation and the analysis process. However, the final decision on the relevance and the presentation of e-evidence to the court is always done by a human (expert).

Referring to the national case law in Lithuania, there was no basis for ethical, moral or processional debates on eligibility and usability of such techniques used in the digital investigation process.

However, according to the National Audit Office of Lithuania audit report "IS cybercrime combated effectively"[970] report, Lithuania is still missing national methodological recommendations for the collection, analysis, preservation, loss or damage assessments of cyber incidents. The guidance document is particularly important for determining the impact of cyber incidents on an organization in relation to a criminal offense and, where necessary, for responding effectively and collecting electronic evidence appropriately.

17.3.2. Organisation of the Pre-Trial Investigation Process

In case of suspicion that a child was compelled to participate in sexual activities, the case is considered as an absolute priority of the national Criminal Police Bureau (hereinafter CPB) and the office of the Lithuanian Prosecutor General[971]. At the early stage of pre-trial investigation, the police initiates involvement of all responsible authorities to ensure that necessary measures are taken to ensure that rights of victims are respected, and that the investigation process is consistent and organised in close collaboration with the experts in the field:

- Forensic experts to appoint forensic examinations to determine the possible biological age of the child being examined. (The qualification of a criminal offense usually depends on the presented conclusion.)

969 https://lkpb.policija.lrv.lt/uploads/lkpb.policija/documents/files/LKPB%202018%20metu%20veiklos%20ataskaita.pdf

970 https://www.vkontrole.lt/failas.aspx?id=4113

971 https://www.prokuraturos.lt/data/public/uploads/2018/03/2018-2020_m_lrgp-strateginis_veiklos_planas.pdf

- The Office of the Inspector of Journalistic Ethics. Pursuant to Article 49 of the Law on Information provides that "the Inspector of Journalistic Ethics shall be accompanied by a group of experts who shall draw conclusions on the classification of press publications, audio-visual works, radio and television programs or programs, websites or other media and / or their content [...] pornographic [...] nature categories "99. Thus, the findings of the Office of the Inspector of Journalistic Ethics in pre-trial investigations regarding the recognition of material as pornographic information are the basis for criminal proceedings in the courts.
- IT professionals to determine if the content is real or created with the help of computer graphics.

A deep analysis of Lithuanian case-law revealed that the most common criminal offenses are images and audio-visual materials containing pornographic content. Accordingly, the Office of the Inspector of Journalistic Ethics usually presents audio-visual materials and images as objects of investigation[972].

Even if the Lithuanian Criminal Police and the Prosecutor General's Office consider as high priority child sexual exploitation cases, and even though procedural and technical instruments are established, nevertheless practically speaking in remote and country side regions some issues can be still identified due to the lack of officer's skills, training, right perception setting or issues arising from very limited resources. It requires time to finalize the shift of work organization in the regions.

17.4. Image Databases

17.4.1. International Child Sexual Exploitation (ISCE) Image and Video Database

International collaboration with INTERPOL and EUROPOL and access to International Child Sexual Exploitation (ICSE) image and video database significantly improved the efficiency of the investigation process of Lithuanian criminal police.

ICSE[973] image and video comparison functionality helps criminal forensics experts to identify connections between victims, abusers and locations in very short period of time. Thanks to ISCE, Lithuanian police can less rely on the competence of external experts and lower the risk of the impact of human errors on the quality of the investigation process.

17.4.2. Europol EC3

Europol's European Cybercrime Centre (EC3) plays an important role by supporting LT police in capability and competence development efforts. EC3 provides regular trainings and hands on workshops using advanced technologies in investigating and combating the sexual crimes against children online.

[972] https://www.bernardinai.lt/2016-12-21-zurnalistu-etikos-inspektoriaus-tarnyba-daugeja-tyrimu-del-pornografijos/

[973] https://www.interpol.int/How-we-work/Databases/International-Child-Sexual-Exploitation-database

Considering that child sexual exploitation is an evolving phenomenon and shaped by developments of technology, professional skills play a crucial role in combating sophisticated crimes.

Lithuanian police continue to innovate and successfully utilize AI based technologies to detect and prevent sexual crimes on the internet. Recently LT police implemented AI based tool for CSEM data analysis. According to LT police, new technologies has a positive impact on the quality and efficiency of criminal investigations and trigger changes in the overall chain of custody.

- ***Challenges:***

However, there are still plenty of opportunities for further improvement. Lithuanian police contain a huge volume of video, criminal images and administrative incidents that could be used to support criminal investigations. Analysis of huge amounts of incidents is very labour intensive and demands highly skilled personnel with the necessary subject matter expertise. Therefore, Lithuanian police are investigating new ways and new technologies that could potentially improve the investigation process.

17.5. Use of Crawlers

Lithuanian police are using certain crawling techniques in specific instances of information gathering operations. However, the exact purpose and efficacy of using such tools is considered confidential.

18. Conclusion

18.1. Summary

This Deliverable D9.4 has presented the legal framework relevant not only for the activities in the course of the GRACE project but also for the use of the GRACE tools and platform after a potential roll-out of the GRACE solution. The both legal frameworks consist of a complex interplay between international and national layers of rules and regulations.

In chapters 2. – 12., the international legal framework has been thoroughly scrutinised by analysing the relevant international treaties at global level of the United Nations as well as at regional level of the Council of Europe. Further, the available rules and regulations at supranational level of the European Union have been examined in-depth.

In chapters 13. – 17. in contrast, the national legal framework in Slovenia, Cyprus, Portugal, Germany and Lithuania have been outlined regarding victims' rights, data protection within the law enforcement ecosystem, the collection and preservation of electronic evidence, the use of image databases and crawlers.

18.2. Evaluation

While there are rather clear and coherent legal frameworks for victims' rights and data protection within the law enforcement ecosystem, the collection and preservation of electronic evidence as well as the use of image databases and search crawlers by law enforcement is still solely determined by national law. This presents a fragmented and challenging background for any technical solution which is to be applied EU-wide. Although the compromise text legislative package regarding Electronic Evidence create hope for improvement, the overall 'bigger picture' requires a high degree of flexibility for the GRACE solution so that the functionalities of its tools and the platform can be adjusted to various mandatory legal requirements at national level.

18.3. Future Work

Background research related to electronic evidence and elements of cross border cooperation has already partly been carried out in the context of producing the Country Reports (see chapters 13. – 17. above). The next step will be to keep monitoring the available legal instruments related to cross border cooperation as well as the cross-border exchange concerning court-proof evidence until the end of the GRACE project.

ANNEX I - GLOSSARY AND ACRONYMS

Term	Definition / Description
CCPCJ	Commission on Crime Prevention and Criminal Justice
CoE	Council of Europe
CSE	Child Sexual Exploitation
CSEM	Child Sexual Exploitation and Abuse Material This document in some cases refers to the term "child pornography". While there is broad consensus that the term "child sexual exploitation material (CSEM)" is significantly more appropriate compared to "child pornography" the latter term was and is still used in legal texts, such as the 2001 Council of Europe Convention on Cybercrime and the 2011 EU Directive 2011/93/EU. When discussion such legal texts, the term "child pornography" instead of CSEM is used. For further information about the discussion about terminology see: Frangez/Klancnik/Karer/Ludvigsen/Konczyk/Perez/Veijalainen/Lewin, The Importance of Terminology Related to Child Sexual Exploitation, published in Revija za kriminalistiko in kriminologijo / Ljubljana 66 / 2015 / 4, page 291–299.
EU	European Union
EPRIS	European Police Records Index System
GDPR	General Data Protection Regulation
JSON	JavaScript Object Notation
LEA	Law Enforcement Agency
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
OSINT	Open Source Intelligence
PDQ	P Divided by Q
REST API	Representational State Transfer Application Programming Interface
TMK+PDQF	video-matching technology
UN	United Nations
UNCAC	United Nations Convention against Corruption
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organized Crime
XML	Extensible Markup Language

Table 3 - Glossary and Acronyms

ANNEX II – OUTLOOK CROSS-BORDER INVESTIGATIONS

Investigating crimes with a cross-border dimension requires specific processes and a close cooperation between LEAs in all the countries involved.[974] Cross-border investigations undertaken unilaterally and therefore without the consent of the competent authorities of the affected countries may violate the fundamental principle of national sovereignty. This principle of international law prohibits countries to carry out investigations within the territory of another country without the permission of the competent local authorities.[975]

Bilateral agreements as well as multilateral agreements such as the United Nations Convention against Transnational Organized Crime (UNTOC)[976] and its three protocols,[977] the Inter-American Convention on Mutual Assistance in Criminal Matters[978] and the European Convention on Mutual Assistance in Criminal Matters[979] provide international/regional solutions for key issues. With Europol the EU Member States have an institutional framework for expedited exchange of information and coordination of investigations.

Right after the publication of the first deliverable (D9.3) the work carried out as part of T9.2 will continue with a focus on cross border cooperation. This component of T9.2 is described in Grant Agreement as follows:

> *„Also, in this task, the analysis of legal issues related to cross-border exchange of court-proof evidence will be tackled. In a first step legal instruments related to cross border cooperation and cross-border exchange will be collected and analysed. This shall include regional (especially EU and CoE instruments), international (especially UNTOC) and bi-lateral agreements. In a second step the requirements (both technical and legal) for court-proof evidence in up to 5 countries will be collected and analysed. Based on the results of the analysis recommendations will be formulated to support the definition of standards protocols, procedures and data formats for international, cross-border approved, information exchange and court proof-evidence.“*

The result of the research will be published in D9.4. Background research related to electronic evidence and elements of cross border cooperation has already partly been carried out in the context of producing the country reports that are part of D9.3.

---

[974] Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[975] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

[976] Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: http://www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

[977] The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition.

[978] Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: http://www.oas.org/juridico/english/sigs/a-55.html.

[979] European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.