The Legislative Framework for Transfers of Personal Data in Cross-Border Criminal Investigations within the European Union

Henna Sarita Hedman
Pro gradu - tutkielma
Oikeusinformatiikka
Oikeustieteen maisteritutkielma
Lapin yliopisto
Syksy 2023
Y28107171

Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: The Legislative Framework for Transfers of Personal Data in Cross-Border Criminal Investigations within the European Union
Tekijä: Henna Sarita Hedman
Koulutusohjelma ja oppiaine: Oikeusinformatiikka
Työn laji: Pro Gradu -tutkielma x Laudaturtyö _ Lisensiaatintyö _ Kirjallinen työ _
Sivumäärä: X + 72
Vuosi: Syksy 2023

ABSTRACT:

The thesis will be examining the legal framework regarding cross-border transfers of data with a focus on personal data in the context of criminal investigations in the European Union (EU).

Different platforms for data sharing will be examined along with the issues arising from the interpretation of international legislation. Provisions governing the different entities conducting transfers of data will be examined and the notion of a 'competent authority' criticized. It is essential to notice that the right for the protection of personal data can be limited on the basis of national security or crime prevention and investigations giving the competent authorities a wider right to process personal data. Hence why one of the key interests of this thesis is to establish the legal framework for the process of requesting and receiving data between authorities in due course of crime investigations. It seems that the law enforcement entities have extensive legal powers to transfer data and the entities which are allowed to process data within the legal framework are not clearly categorized. New predictive policing technologies are posing a risk for the EU data protection laws to be interpreted too broadly nationally.

Keywords: Law enforcement; EU crime prevention; personal data; material scope; information relating to; cross-border data transfers; international agreements; competent authority; police information exchange; data protection law; national security.

Table of Contents

BIBLIOGRAPHY

Textbooks:

Bygrave, Lee, Data Protection Law: Approaching Its Rationale, Logic and Limits. Springer Netherlands 2002.

Craig, Paul – de Búrca, Gráinne, EU Law: Texts, Cases and Materials. Seventh Edition, Oxford University Press 2020.

Fredman, Markku – Kanerva, Janne – Tolvanen, Matti – Viitanen Marko, Esitutkinta ja pakkokeinot. Alma Talent 2020. 6. painos.

González Fuster, Gloria, The Emergence of Personal Data Protection as a Fundamental Right of the EU, vol 16. Springer International Publishing 2014.

Gutiérrez Zarza, Ángeles, Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe. Springer 2015.

Hijmans, Hielke, The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU. Springer Int Publishing 2016.

Hirvonen, Ari, Mitkä metodit?. Yleisen oikeustieteen julkaisuja 2011.

Korpisaari, Päivi – Pitkänen, Olli – Warma-Lehtinen, Eija, Tietosuoja. Alma Talent 2022.

Kosta, Eleni – Leenes, Ronald and many more, Research Handbook on EU Data Protection Law. Edward Elgar Publishing 2022.

Lohse, Mikael, Johdatus tiedusteluun. Alma Talent Oy 2019.

Lynskey, Orla, The Foundations of EU Data Protection Law. OUP 2016.

Mitsilegas, Valsamis, EU Criminal Law. Hart Publishing 2009.

Naef, Tobias, Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law. Springer European Yearbook of International Economic Law 2022.

Sharma, Sanjay – Menon, Pranav: Data Privacy and GDPR Handbook. John Wiley & Sons 1st edition 2020.

Storey, Tony – Turner, Chris, Unlocking EU Law. 3rd edition. 2011 Hodder Education.

Tzanou, Maria, The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance. Hart Publishing 2017.

Articles and reports:

Bárd, Petra, CEPS Paper in Liberty and Security in Europe (2018).

Bygrave, Lee, Data Protection Law: Approaching Its Rationale, Logic and Limits (Springer Netherlands 2002).

Carrera, Sergio – Stefan, Marco – Mitsilegas, Valsamis, 'Report of CEPS and QMUL Task Force: Cross-border data access in criminal proceedings and the future of digital justice – Navigation the current legal framework and exploring ways forward within the EU and across the Atlantic', Centre for European Policy Studies, 10/2020.

Caruana, Mireille, 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2019) 33(3) Int Rev Law Comput Tech 249.

Crespi, Serenam 'The applicability of Schrems principles to the Member States: national security and data protection within the EU context', E.L. Rev. 2018, 43(5), 669-686.

González Fuster, Gloria, 'Curtailing a Right in Flux: Restrictions of the Right to Personal Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), Hacia un nuevo derecho europeo de protección de datos (2015).

Jeanne Pia Mifsud Bonnici, 'Exploring the Non-Absolute Nature of the Right to Data Protection' 28 International Review of Law, 2014, Computers & Technology 131.

Kranenborg, Herke, '*Commentary on Article 2 Material Scope*' in Kuner, Christopher, Bygrave, Lee A and Docksey, Christopher (eds) The EU General Data Protection Regulation: A Commentary (OUP 2020).

Lynskey, Orla, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing', 15(2) International Journal of Law in Context 162 2019.

Opinion of the European Data Protection Supervisor on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (2007/C 169/02).

Purtova, Nadezhda, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, 018 Law, Innovation and Technology 10(1), (2018). Online access. SSRN. [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355]. Accessed 15.07.2023.

Sirius EU Digital Evidence Situation Report, 22 December 2022, European Union Agency for Law Enforcement Cooperation 2022, Europol, Eurojust and the European Judicial Network (EJN).

Taylor, Linnet, What is data justice? The case for connecting digital rights and freedoms globally. Tilburg Institute for Law, Technology and Society (2017). Online access: [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918779]. Accessed 15.07. 2023.

Wahl, Thomas, Civil Rights Organisations Criticise Prüm II Proposal. Eucrim, 5 October 2022.

European Commission proposals and Council Recommendations:

Commission on the Terrorism Finance Tracking System (TFTS) in the European Union, COM (2013) 842.

Council conclusions on mutual recognition in criminal matters 'Promoting mutual recognition by enhancing mutual trust' (2018/C 449/02).

Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation ST/8720/2022/INIT, OJ L 158, 13.6.2022*, p. 53–64.*

Proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 2011/0023 (COD) (Commission on the EU Passenger Name Record (PNR)).

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, Brussels, 8.12.2021, COM(2021) 784 final, 2021/0410(COD).

Council Decisions:

Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100 (The Swedish Initiative).

Council of Europe Convention on Mutual Assistance in Criminal Matters and its Protocols ('1959 MLA Convention').

EU Legislation:

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, OJ L 8, 13.1.2010, p. 11–16.

Charter of Fundamental Rights of the European Union, 2000/C 364/01.

Consolidated text: 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, original OJ L 135, 24.5.2016, p. 54-114. (Europol Regulation (2016/794)).

Consolidated text: 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, original OJ L 135, 24.5.2016, p. 54-114.

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 exe- cution of criminal penalties, and on the free

movement of such data, and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5.2016.

Directive (EU) 2016/680 the data protection law enforcement directive.

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 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, PE/3/2023/REV/1, OJ L 191, 28.7.2023.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 31.7.2002.

Directive 2012/13/EU on the right to information in criminal proceedings, OJ L 142, 1.6.2012.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

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 [1995] OJ L281/31.

EU Information Management Strategy, 5307/2/17 REV 2.

General Data Protection Regulation (EU) 2016/679.

OJ C 53, 3.3.2005.

Programme of Measures to implement the principle of mutual recognition of decisions in criminal matters. OJ C 12, 15.1.2002.

Regulation (EC) No 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) (codification), OJ L 77, 23.3.2016.

Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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 (Text with EEA relevance.). PE/31/2018/REV/1. OJ L 295, 21.11.2018.

Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of such data.

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA. PE/37/2018/REV/1. OJ L 295, 21.11.2018.

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, PE/4/2023/REV/1, OJ L 191, 28.7.2023

Schengen Agreement (Sops 23/2001).

The Hague Programme: strengthening freedom, security and justice in the European Union

Conventions:

Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations. Official Journal C 024 , 23/01/1998, p. 0002 – 0022.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

Convention Implementing the Schengen Agreement, and the 2000 Convention on Mutual Legal Assistance in Criminal Matters between the Member States (‘2000 EU MLA Convention’) and its Protocol.

Treaties:

Treaty on European Union, OJ C 326, 26.10.2012, p. 13–390.

Treaty on the Functioning of the EU, OJ C 326, 26.10.2012, p. 47–390.

Treaty of Lisbon OJ C 306,17.12.2007, p. 1-271.

Treaty of Maastricht, 07.02.1992.

Vienna Action Plan 1998.

Finnish national legislation:

Act on amending the law on transport services (301/2018).

Act on the Administration of the Border Guard (577/2005).

Act on the European Union Law Enforcement Cooperation Agency (2017/214).

Act on the Processing of Personal Data by the Border Guard (639/2019).

Act on the Processing of Personal Data by the Customs (650/2019).

Act on the Processing of Personal Data by the Police (616/2019).

Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018).

Act on the Processing of Personal Data in Police Work (761/2003).

Border Guard Act (578/2005).

Finnish Police Act (872/2011).

Laki Belgian kuningaskunnan, Saksan liittotasavallan, Espanjan kuningaskunnan, Raskan tasavallan, Luxemburgin suurherttuakunnan, Alankomaiden kuningaskunnan ja Itävallan tasavallan välillä rajat ylittävän yhteistyön tehostamisesta erityisesti terrorismin, rajat ylittävän rikollisuuden ja laittoman muuttoliikkeen torjumiseksi tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä sopimuksen soveltamisesta (277/2007). English translation: The Act on enhancing cross-border cooperation between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the Republic of Germany, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, and the Republic of Austria, in particular on the enactment of provisions falling within the scope of the legislation of the Agreement on Combating Terrorism, Cross-Border Crime and Illegal Migration, a and on the application of the Agreement (277/2007).

Laki Belgian kuningaskunnan, Saksan liittotasavallan, Espanjan kuningaskunnan, Raskan tasavallan, Luxemburgin suurherttuakunnan, Alankomaiden kuningaskunnan ja Itävallan tasavallan välillä rajat ylittävän yhteistyön tehostamisesta erityisesti terrorismin, rajat ylittävän rikollisuuden ja laittoman muuttoliikkeen torjumiseksi tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä sopimuksen soveltamisesta annetun lain muuttamisesta (1208/2011). English translation: The Act on enhancing cross-border cooperation between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the

Republic of Austria, in particular on the enactment of provisions falling within the scope of the legislation of the Agreement on Combating Terrorism, Cross-Border Crime and Illegal Migration, and amending the Act on the Application of the Agreement (1208/2011).

Laki Euroopan Unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta tehdyn neuvoston puitepäätöksen lainsäädännönalaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäätöksen soveltamisesta (26/2009). English Translation: Act on the national implementation and application of the provisions of the framework decision of the Council on simplifying the exchange of information and intelligence between the law enforcement authorities of the member states of the European Union (26/2009).

Law on the implementation of certain provisions of the decision on Europol (563/2011).

Maritime Search and Rescue Act (1145/2001).

Personal Data Act (471/1987).

Personal Data Act (523/1999).

Dissertations and theses:

Keskinen, Nina, Kansainvälinen virka-apu ja poliisin kansainvälinen tiedonvaihto. Pro Gradu-tutkielma 2008.

Kurvinen, Evgeniya, Suomen ja venäjän viranomaisten välinen tietojenvaihto ja sen sääntely. Dissertation. University of Eastern Finland 2021.

Government proposals:

HE 243/2006.

HE 31/2018 vp.

Cases:

Amann v Sitzerland App no 27798/95 (ECtHR, 16 February 2000).

Breyer v Bundesrepublik Deutschland, Case C-582/14, EU:C:2016:779.

Criminal Proceedings against Maria Pupino [2005], Case C-105/03, ECR I-5285.

Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987).

Niemietz v Germany App no 13710/88 (ECtHR, 16 December 1992).
Schrems v Data Protection Commissioner, Case C-362/14 (European Court of Justice 2015).
Van Gen den Loos v Netherlands Inland Revenue Administration. 07/03/1985 European Court Reports 1985 -00779 ECLI identifier: ECLI:EU:C:1985:104.

Online sources:

Council of Europe on Details of Treaty No. 108. [https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108]. Accessed 17.05.2023.

Dr. Toom, Victor June, Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision: LIBE Committee Study, 2018. [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018) 604971_EN.pdf]. Accessed 20.03.2023.

Eurojust. Eurojust.europa.eu. [https://www.eurojust.europa.eu/about-us]. Accessed 15.01.2023.

European Commission - Fact Sheet Questions and Answers - Data protection reform package, What about the Data Protection Directive for the police and criminal justice sector? [http://europa.eu/rapid/press-release_MEMO -17-1441_en.htm]. Accessed 01.04.2023.

European Commission on E-evidence: https://commission.europa.eu/law/cross-border-[cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en]. Accessed 30.06.2023

European Commission, SIRENE Cooperation. [https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation_en]. Accessed 25.04.2023.

European Commission: e-Evidence: Commission welcomes political agreement to strengthen cross-border access for criminal investigations 29.10.2022. [https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7246]. Accessed 04.06.2023.

European Commission: Security Union: Commission facilitates access to electronic evidence. [https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343]. Accessed on 04.06.2023.

European Data Protection Supervisor, Annual Report 2022. P.2. edps.europa.eu. [https://edps.europa.eu/system/files/2023-04/23-04-26_edps_ar_2022_annual-report_en.pdf]. Accessed 11.03.2023.

European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022. Accessed 10.03.2023.

European Union Agency for Criminal Justice Cooperation, European Investigation Order: [https://www.eurojust.europa.eu]. Accessed 15.01.2023.

European Union on European Commission. Europa.eu. [https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/european-commission_en]. Accessed 04.04.2023.

Interpol. Interpol.int. [https://www.interpol.int/Who-we-are/Legal-framework/Data-protection]. Accessed 15.01.2023.

Ministry of the Interior, Effectiveness of the new Act on the Processing of Personal Data by the Police to be assessed 22.04.2021. [https://intermin.fi/en/-/effectiveness-of-the-new-act-on-the-processing-of-personal-data-by-the-police-to-be-assessed]. Accessed 10.06.2023.

Savolainen, Jukka, EU:n neuvostolta kaksi yleisnäkemystä ja suositus operatiivisen poliisiyhteistyön ja tietojenvaihdon parantamiseksi. Edilex toimitus 14.06.2022. [https://www-edilex-fi.ezproxy.ulapland.fi/uutiset/76778?allWords=eu+neuvostolta+kaksi+n&offset=1&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=1448297]. Accessed 01.03.2023.

Wahl, Thomas, 'Civil Rights Organisations Criticise Prüm II Proposal'. Eucrim, 5 October 2022. Eucrim.eu. [https://eucrim.eu/news/civil-rights-organisations-criticise-prum-ii-proposal/]. Accessed 18.05.2023.

ABBREVIATIONS

AI	Artificial Intelligence.
CCF	Commission for the Control of INTERPOL's Files.
CFR	Charter of Fundamental Rights of the European Union.
CoE	Council of Europe.
DPD	Data Protection Directive.
EAW	European Arrest Warrant.
ECtHR	European Court of Human Rights.
EIO	European Investigation Order.
EIS	European Information System of the European Police Agency.
EJCN	European Judicial Cybercrime Network.
EJN	European Judicial Network.
EU	European Union.
GDPR	General Data Protection Regulation.
Ibid.	Latin: Ibidem, in the same place.
IGO	Inter-Governmental Organization.
IM	EU Information Management Strategy.
LED	Law Enforcement Directive.
NBI	National Bureau of Investigation.
NGO	Non-Governmental Organization.
OSP	Online Service Provider.
SIENA	The Secure Information Exchange Network Application.
TEU	Treaty on European Union.
TFEU	Treaty on the Functioning of the EU.
VR/AR	Virtual/Augmented Reality.

1. INTRODUCTION

1.1. Research problem

European Union (EU) Criminal law covers measures which have a great impact on the protection of fundamental rights and the relationship between an individual and the State. The amount of cross-border data flow has been increasing tremendously in the recent decade. It seems that data transfer requests in the EU are being used in over half of all criminal investigations to gather evidence of the suspect. This can be said to have elevated privacy risks in terms of authorities sending data beyond the legal limit. What makes a request cross-border is when the investigation is commencing in one country and the entity receiving the request and furthermore complying with or rejecting it is in another.

This research is within the area of legal informatics and shall be a comparative assessment of privacy issues in the context of exchange of information between 'competent authorities'. The study will analyze the legal framework within the EU governing processing of data by law enforcement entities who are responsible for participating and executing cross-border data transfers – specifically personal data in crime investigations. Processing has been defined in Article 3(2) LED and Article 4(2) GDPR as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

Furthermore, the purpose of the analysis is to ascertain the needs for legal reforms and how the accessibility to data can be ensured without unjustifiably interfering with an individual's basic rights of those whose personal data is or may be transferred to another country. When determining the entities processing personal data in criminal matters, the platforms for data exchange shall be examined as well. This study will critically assess cross-border data transfer legislation and whether data transfers interfere with the integrity of EU criminal law questioning the safeguards purported to ensure that data protection legislation is indeed complied.

Although the EU legislator has attempted to separate the different data protection regimes in the context of law enforcement, there are arguments regarding the General Data Protection Regulation (GDPR, 2016/679) and the Directive (LED, 2016/680)[1], not being dichotomous as they are not fully exclusive. Issues regarding this shall be examined further later in Chapter 3.5.

1.2. Question layout

The main question that this thesis purports to answer is how data is transferred across borders and what is the legislative framework for such transfers in a criminal law context. For these purposes it is important to understand the development of the EU instruments governing cross-border data transfers.

The different categories of data are often held by cross border service providers.[2] To withhold the rule of law within the EU criminal justice area, the systematic ex ante involvement of competent judicial authorities is essential to maintain trust between the Member States.[3] The research will give an historical overview on how data protection legislation started to take the current form starting from being a fundamental right under Article 8 of the European Convention on Human Rights (ECHR) and dives into a discussion on how the set of legislation relates with right to privacy and on how the EU secondary law is linked to data protection.

There are available remedies concerning the cross-border data transfers in criminal proceedings. They rely upon judicial control and the intervention of competent authorities of transferring and receiving countries. Hence, the correct application of EU procedural rights is examined in the material. The law enforcement measures when transferring data to third countries must undergo higher judicial scrutiny.[4] When authorities operate in different criminal justice systems, 'conflicts of laws can be exacerbated by instruments that promote direct and unmediated extraterritorial enforcement of criminal jurisdiction.'[5] Data transfers in different criminal justice systems for the purposes of this thesis shall refer to the justice

[1] Directive (EU) (2016/680).
[2] Carrera – Stefan – Valsamis 2020, p. i.
[3] *Ibid…*
[4] *Ibid…*
[5] *Ibid…*

systems of the Member States. Data transfers to third countries will not be examined in this thesis.

It is evident that data protection and personal data processing impacts us all individually but also as a society.[6] *Rodotá* has stated that the nature of a democratic society is measured by the extent to which personal data is protected.[7] It is crucial that processing of data is conducted with respect to the established fundamental principles such as necessity and proportionality.

The European Commission (EC), which is the body of the European Union (EU) is responsible for drawing up legislative proposals in the EU.[8] It has been proposing new legislations on many areas which will have or have already had an impact on data protection as a legal field and its secondary legislation. *Kosta* and *Leenes* are calling this phenomenon 'acti-fication'.[9] The question is, what do all the new instruments add to the European Data Protection laws and what is their impact of data transfers in cross border criminal investigations and prevention of cross-border crime.

The LED[10], which was created for 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 the execution of criminal penalties, and on the free movement of such data has conflicting legislative provisions with the GDPR.[11]

This research will provide a thorough examination of the legal framework of the GDPR and the LED but also the legislative framework as a whole. The relevant authorities which are explained in this thesis are selected on the basis of the Finnish law enforcement authorities that conduct the necessary data requests and transfers.

---

[6] Kosta – Leenes – Kamara 2022, p. 1.
[7] Rodotá 2009.
[8] European Union on European Commission. Europa.eu: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/european-commission_en.
[9] Kosta – Leenes – Kamara 2022, p. 2.
[10] 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 OJ L119/89 4.5.2016
[11] *Ibid.*, p. 3.

1.3. Delimitations and margins of the research

The analysis will be focusing solely on operational approach and will assess the relevant national norms, EU legislation, International Agreements and Treaties governing exchange of personal information in criminal law context. No strategic information of the law enforcement will be analyzed in this thesis.

The GDPR's notion of 'public interest' will be examined only in regard to criminal proceeding and prevention of crime, and on how it gives the authorities the right to demand information and digital evidence. No information related on transfers of data to the third world countries are further analyzed.

1.4. Methods of the research

As one of the purposes of this thesis is to clarify the legal and operational framework for cross-border data transferring, the method of jurisprudence and legality are most suitable. The purpose is to interpret scattered laws, provisions and directions to conclude how the law should be interpreted. Analogical approach will be taken to lay the foundation to data transfer matters in the EU and an overview of how the modern-day rules have developed to this day.

A value-based interpretation of the relevant rules highlighting the general principles of law and human rights will be implemented. Relevant norms, doctrines of law, jurisprudence theories and the legal order will be analyzed through a systematic approach.

1.5. Jurisprudential and social relevancy of the research

As the criminal justice system and the issues relating to data transfers are becoming more and more international, the development of legislation concerning this specific area of legal instruments may not keep up with the need for clear rules and structure. There has been an increasing need to exchange information in order to investigate and prevent cross-border crime in the past decade.[12] For this reason there has been an adaptation of mutual principles across the EU, slowly strengthening the policy for working together cross-borders.

[12] Gutierréz 2015, p. 3.

Mutual recognition provides that judicial authorities are entitled to contact each other directly to exchange information as opposed to the fact that previously this cooperation used to be in the hands of the diplomatic services of the Member States. This direct contact and change of information must of course follow the current legal framework.[13] According to the principle of availability initiated by The Hague Program, a law enforcement officer needing information to thoroughly investigate, should be able to gain access to the necessary data from another Member State. The principle is one of the fundamental reasons why information systems and tools have developed to exchange information.[14]

This analysis shall explore with a comparative approach the different statues, treaties and rules concerning international data transfers in criminal proceedings and different ways on co-operation, making the research jurisprudentially and socially relevant in this fastly growing area of law.

[13] Gutierréz 2015, p. 3.
[14] *Ibid.*, p. 3–4.

2. PARTIES, OBJECT, AND METHOD OF EXCHANGE OF PERSONAL DATA IN THE CONTEXT OF CRIMINAL PROCEEDINGS

2.1. Authorities

The subject of this thesis is cross-border exchange of information and more specifically exchange of personal data in cross-border crime investigations in the EU. The thesis examines the transfer and processing of data between law enforcement authorities. The authority that can handle personal data in those situations is determined in the current legislation or referred to in international agreements.

Authority in Finland has been defined as being a public entity which can use public power and has been selected through a special procedure.[15] An authority has a special responsibility as an official of the government. This is called the civil service principle. The purpose of this principle is to ensure the legality, uniformity, and objectivity of decision-making. The principle is partially based on the idea that administrative tasks involving the exercise of power require special expertise and training. [16] Civil service status and official responsibility are thought to ensure this.

The authorities which take part in processing and transferring of personal data in the context of crime investigation and crime prevention are the police, Interpol, Europol, Border Security Control, and Customs.[17] According to the Finnish Criminal Investigation Act (805/2011, amendments to 736/2015 included) Chapter 2, section 1 subsection 1, the preliminary investigations are carried out by the police. The police are regarded as the general preliminary investigation authority. Other special preliminary investigation authorities are the Border Security Control, military, and customs authorities.

When it comes to cross-border data transfers for the purposes of crime investigation, the receiving and sending parties are referred to as competent authorities. A competent authority

[15] Mäenpää 2017, p. 26.
[16] *Ibid*…
[17] HE 31/2018 vp, s. 35–36.

for these purposes is defined in the Finnish Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018).

According to Section 3, subsection 5 of the Act, a competent authority means any public authority competent for the prevention, detection, investigation, referral for consideration of charges, consideration of charges or other activities relating to the prosecution of criminal offences, conviction and sentencing or the execution of criminal penalties, including safeguarding against and preventing threats to public security, as well as the Defence Forces, the police and the Border Guard when performing duties referred to in section 1, subsection 2.[18] These duties are for a consideration of charges and other activities of prosecutors in relation to a criminal offence.

The exercise of public power must be based on law.[19] The definition of the tasks of authorities does not include general authority for the use of public power which is deemed necessary to carry out missions or tasks. Hence, the use of public power by the police is based on special provisions.[20]

The tasks and powers of the police are defined by a broad and flexible general provision in the Finnish Police Act (872/2011). According to the Finnish Police Act section 1, the duty of the police is to secure the rule of law, maintain public order and security, prevent, detect, and investigate crimes, and submit cases to prosecutors for the consideration of charges. The police cooperates with other public authorities and with communities and residents in order to maintain security, and they engage in international cooperation pertaining to their duties. The police can use direct public power and intervene with another's interest.[21] Therefore, many legal acts give the police direct authority to access one's data. Some of these specific authorities and their access to retrieve and process data shall be examined next.

2.1.1. Europol

It is stated in K.1(9) article of the Treaty of Maastricht[22] that Europol is an EU wide information exchange system. In official terms it is called the European Union Agency for

[18] Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018).
[19] Mäenpää 2017, p. 276.
[20] *Ibid*...
[21] *Ibid.*, p. 25.
[22] The Treaty of Maastricht, 07.02.1992.

Law Enforcement Cooperation.[23] All Member States of the EU take part in the functions of Europol and Interpol. Europol became an EU bureau by Council Decision on Europol (2009/371/YOS).

Europol's goal is to strengthen the cooperation of national law enforcement entities in their mission of combatting international serious crime and terrorism. At the center of Europol's focus is its purpose to enhance the exchange of data between the national authorities of the Member States.

It is defined in Article 2(a) of the Europol Regulation (2016/794)[24] that a competent authority refers to all police authorities and other law enforcement services existing in Member States which have the responsibility to prevent and combat criminal offences. The contact center for Europol on a national level is the National Bureau of Investigation (NBI).[25] NBI exchanges information with not only Europol but with the other Member States.

Europol is an international law enforcement agency analyzing and exchanging criminal intelligence information.[26] Operational analysis as a term contains all methods and techniques that are implemented to collect, store, process and assess information.[27]

According to Article 4(1)(a) of the Regulation[28] Europol shall collect, store, process, analyze and exchange information, including criminal intelligence. It shall support Member States in processing data provided by other countries.[29] The data which Europol can process must be provided for it. This means that Member States, Union entities or private parties or persons shall provide data to Europol according to their national law and Article 7.[30] Europol may, however, retrieve and process information from publicly available sources.[31] Only duly authorized staff may gain access or retrieve and process data from Union or other systems if

[23] Europol Regulation (2016/794), Article 1(1).
[24] *Ibid*…
[25] Law on the implementation of certain provisions of the decision on Europol (563/2011), 3 §.
[26] Helminen – Kuusimäki – Rantaeskola 2012, p. 167.
[27] Europol Regulation (2016/794), Article 2(b)
[28] *Ibid*…
[29] *Ibid.*, Article 4(1)(h).
[30] *Ibid.*, Article 17(1)(a-c).
[31] *Ibid.*., Article 17(2).

it is necessary for a certain task. This must be achieved so far as it is necessary and proportionate for the task at hand.[32]

Europol can access personal information for the purposes of crime investigation solely. The term 'purposes' for data processing means cross-checking information about suspects that are suspected to have committed or have already been convicted of a criminal offence. The crime must fall within Europol's objectives.[33] Europol can also process data of persons who are reasonably believed to be committing criminal offences[34] or when they need to inform the suspect or public about a wanted person. Data processing may also occur for the purposes of research, operational analyses or when Europol functions as a facilitator when Member States exchange information.[35] Processing data for analyzing purposes shall happen within the framework that the Executive Director of the time defines.[36]

Data processing must always be necessary and proportionate.[37] It must be conducted to gain information for a specific criminal investigation and for a certain purpose.[38] It is on the Member State providing the information which must determine the purpose for which that information shall be processed.[39]

2.1.2. Interpol

Interpol is short for International Criminal Police Organization, and it is the oldest international policing organization.[40] According to *Helminen* and *Kuusimäki,* since it has not been established by an international convention, it is as an organization located between inter-governmental organization (IGO) and non-governmental organization (NGO). From the beginning of its creation one of its main goals has been sharing information between the policing authorities of the Member States and collecting intelligence about international crime.[41] Data protection in Interpol is supervised by a special supervisory authority called

[32] Europol Regulation (2016/794), Article 17(3).
[33] *Ibid.*, Article 18(2)(f).
[34] *Ibid.,* Article 18(2)(a)(i-ii).
[35] *Ibid.*, Article 18(2)(b-e).
[36] *Ibid*, Article 18(3).
[37] *Ibid*, Article 18a.
[38] *Ibid*, Article 18a(3).
[39] *Ibid*., Article 19.
[40] Helminen, Klaus – Kuusimäki, Matti – Rantaeskola, Satu, Poliisilaki. 2012 Alma Talent Oy, p. 165.
[41] Keskinen 2008.

the CCF (Commission for the Control of Interpol's files).[42] The organization does not have its own international cross-border authorities but each Member State's national authorities conduct their practices by interpreting national legislation.

Exchange of information is always conducted by national offices. In Finland it is the NBI.

2.1.3. Eurojust

Eurojust was established in 2002 and it is an official entity of the EU. According to the Eurojust Regulation[43] it is an entity in which prosecutors and investigators operate together in order to prevent cross-border crime. It can request information from a Member State, start investigations and develop prosecutorial strategies.[44] Only national members and their assistance personnel have access to their data base which holds personal information.[45] The purpose of their data base is to monitor the lawfulness of processing conducted by the Europol and its compliance with the data protection rules.[46] The Executive Board appoints a Data Protection Officer, a supervisory authority, who monitors the lawfulness of processing.[47] Everyone has the right to access their personal information to see what information is being kept about them and request Eurojust to delete or fix their information.

A new data protection regime for Eurojust was introduced with the application of the Regulation 2018/1725[48]. This Regulation is meant to be interpreted homogenously with the GDPR[49] whenever the provisions follow the same principles.[50] Regulation 2018/1725 differs from the GDPR in that sense that it applies to Union's bodies, institutions, offices and agencies.[51] Rules in Regulation 2018/1725 must also be consistent with the LED to prevent divergencies which may be hampering the exchange of personal data between the Union entities when carrying activities falling within the scope Chapter 4 or 5 Title V of the Treaty on the Functioning of the European Union (TFEU)[52] which governs judicial operation in

[42] Interpol.int. Section 'Data Protection'. Accessed 15.01.2023.
[43] Regulation (EU) (2018/1727). Consolidated version 01.06.2022, Article 2.
[44] Eurojust.europa.eu. Section 'About us'. Accessed 15.01.2023.
[45] Helminen – Kuusimäki – Rantaeskola 2012, p. 170.
[46] Regulation (2018/1727), p. 138–183. Consolidated version 01.06.2022, Article 23.
[47] *Ibid.*, Article 16(l).
[48]Regulation (2018/1725), p. 39–98.
[49] Regulation (2016/679), p. 1–88.
[50] Regulation (2018/1725), Recital 5.
[51] *Ibid…*
[52] Consolidated version of the Treaty on the Functioning of the European Union, p. 47–390.

criminal matters and police cooperation.[53] The GDPR and the LED shall be examined in further depth in Chapter 3.5.

Regulation 2018/1725 Article 4(a) requires that processing of personal data is lawful, fair, and transparent. It must be collected for specified purposes and be accurate (purpose limitation). When the processing of personal data covers processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes it is not considered incompatible with the initial purposes for processing personal data. Identification of the subject must not be identifiable for no longer that is necessary. Eurojust may process personal data that reveals ethnic origin, political opinions, religious belief, biometric data with consent and when the processing is essentially necessary for substantial public interest, according to Article 10.

2.1.4. Border Security Control

Border Security is one of the safety authorities maintaining border security. Border security is defined in the Border Guard Act (578/2005) Section 2(6). Border security means measures taken in Finland and abroad to prevent breaches of provisions when national borders are crossed. It also refers to the measures taken to prevent threats to the public order and security posed by the cross-border passenger traffic. In essence the Border Guard combats cross-border crime, and its goal is to ensure the safety of crossings at the border. Its governance is provisioned by the Act on the Administration of the Border Guard (577/2005). The internal order can be compared to be military like.[54] Officials who work in military positions are subjected to Chapter 45 of the Criminal Code (39/1889) which consists of the military crimes. The Aliens Act (301/2004) governs those tasks relevant to immigration.

The provisions related on the processing of personal data and on the right to obtain and disclose personal data while carrying out the duties of the Border Guard are found in the Border Guard Act (578/2005), the Act on the Processing of Personal Data by the Border Guard (639/2019), and the Maritime Search and Rescue Act (1145/2001).

[53] Regulation (EU) 2018/1725, Recital 5.
[54] Helminen – Kuusimäki – Rantaeskola 2012, p. 123.

The GDPR applies to the Border Guard also in relation to the processing of personal data.[55] The Act on the Processing of Personal Data by the Border Guard (639/2019) applies to Border Guard in terms of processing of personal data for the purposes of preventing, detecting, and investigating offences, referring them for consideration of charges, safeguarding against threats to public security and preventing such threats, protecting natural security and in military administration of justice.[56]

The Act on the Processing of Personal Data by the Border Guard (639/2019) applies to the processing of personal data by the Border Guard where the processing is partly or fully performed by automated means, or the data forms a filing system or a part thereof.[57] The processing must follow the general principles of necessity and proportionality. It must comply with the purpose limitation and should not without an acceptable reason be based on specific characteristics of that person such as origin.[58]

The Border Guard on the basis of Section 6[59] can process basic personal data in border control to maintain security and order at the border (Section 7) or if the person is suspected of an offence[60], is a subject of a criminal investigation[61], reports an offence or is an injured party[62], a witness[63], a victim[64] or some other source relating to the duty[65]. The Border guard has evidently a broad authority to access personal data while performing cross-border duties. When interpreting the above, it is evident that according to the provisions governing the processing of personal data, the Border Guard may access personal data almost as long as it has an interest to do so.

Of course, the Border Guard does play a big part in preventing for example illegal drug smuggling to Finland which is why their wide access to the data bases is crucial in terms of preventing crime and for it to be effective. It is important that the Border Guard officers are not reluctant to complete certain tasks in the fear of committing data breaches.

[55] The Act on the Processing of Personal Data by the Border Guard (639/2019), Section 2.
[56] *Ibid.*, Section 2(1).
[57] *Ibid.*, Section 1(1-2).
[58] *Ibid.*, Section 3.
[59] *Ibid.,* Section 6.
[60] *Ibid.,* Section 8(1-2).
[61] *Ibid.,* Section 8(3).
[62] *Ibid.,* Section 8(4).
[63] *Ibid.,* Section 8(5)
[64] *Ibid.,* Section 8(6).
[65] *Ibid.,* Section8(7).

The Border Guard is permitted by the Act to process data for the protection of public security and safety personal by processing identifying characteristics such as biometric data[66] and identification information on a decision by the prosecutor or court and information on convictions, waived charges, and information on whether a decision is final.[67]

For the purposes of preventing and detecting offences the Border Guard can process personal data if there are reasonable grounds to believe the person has committed or intends on committing an offence for which the maximum punishment is imprisonment.[68] If a person may be linked to the person of interest, the Border Guard may process their personal data also.[69] Border Guard may essentially base the processing of data on security and safety of the border and on the purpose of preventing and detecting offences.

2.2. Digital platforms for data exchange in criminal matters

2.2.1. SIENA

The Secure Information Exchange Network Application (SIENA) is a highly secured information exchange channel. Information can be exchanged by the police, Border Security Control and Customs.[70] From the different platforms SIENA serves the best at delivering intelligence.[71] Sharing information happens automatically from information systems to Europol's databases through SIENA.

Although the system is used for data sharing, there is certainly direct communication between different authorities also, but this kind of communication must always be approved by the NBI.

[66] The Act on the Processing of Personal Data by the Border Guard (639/2019), Section 9(2).
[67] *Ibid.*, Section 9(4).
[68] *Ibid.,* Section 10(1).
[69] *Ibid.*, Section 10(2).
[70] Helminen – Kuusimäki – Rantaeskola 2012, p. 169.
[71] *Ibid...*

2.2.2. EIS

EIS is an information system of the European Police Agency. The Member States enter information to EIS regarding information on criminal cases under Europol's jurisdiction.

EIS enables to combine all the relevant information concerning criminals making it easier to connect their activities and connections.[72] All the national legislation concerning Europol's databases is based on Act on the European Union Law Enforcement Cooperation Agency (2017/214) repealing the Act on the implementation of Certain Provisions of the Decision on Europol (563/2011) and the Europol Regulation (2016/794).

2.2.3. VIS

VIS stands for Visa Information System, and it is an EU information system. The goal of this system is to enhance the mutual visa politics and prevent illegal immigration by easing border checks.[73] Provisions for VIS and its establishing regulation is Regulation (EC) No 767/2008. Personal data can be stored in VIS for a maximum of five years (principle of necessity). A shorter period would not be sufficient for the purposes of being able to consider previous visas upon a decision of the right to enter.[74] The National Supervisory Authorities are responsible for monitoring the lawfulness of the processing of personal data.[75] According to Article 3 subsection Europol can have access to VIS if it is necessary to perform their tasks.

Regulation (EC) No 2016/399 recommends that the Border Guard should use all of the information in the VIS such as biometric data for entry checks at the external borders.[76] Data from VIS can be made available to or transferred to a third party or international organization for the purposes of the prevention and detection of terrorist offences and of other serious offences according to Article 3 subsection 3. It is the competent visa authorities that shall have access to consult data in VIS. Border Guard is one of these authorities.

[72] Helminen – Kuusimäki – Rantaeskola 2012, p. 169.
[73] Regulation (EC) No (767/2008), Recitals 1-5.
[74] *Ibid.,* Recital 14.
[75] *Ibid.,* Recital 19.
[76] Regulation (EC) No (767/2008), Recitals 11-14.

2.2.4. SIS and SIRENE

Cooperation in police matters is governed by Section III Chapter 1 of the Schengen Agreement (Sops 23/2001). According to this agreement, the parties commit that their police officers will provide aid to each other to prevent and investigate crime. All functions must abide national laws and authoritative powers.

Schengen Information System (SIS) is an information system. SIS is not a separate authority entity.[77] It consists of a mutually held technical support stations called CSIS and national stations (NSIS). Every Member State that is a party to the agreement shall also set up a SIRENE office. SIRENE offices are responsible of coordinating activities in relation to alerts by SIS and the information exchanges. It must operate around the clock.[78] SIS functions 24/7 and is allocated in the NBI. All the notifications to SIS go through SIRENE and their compliance with the Schengen provisions and national laws are reviewed.[79]

What information can be saved in SIS can be found in Article 94(3) of the Schengen Agreement. The information refers to general information on nationality[80], names[81], whether the person is violent or holds weapons[82] and other general information. Data processing of personal data must follow what is stated in Article 126 of protection of personal data. According to subsection 1 there must be sufficient national safeguards and the processing must follow the general principles of data processing.

2.2.5. E-evidence

It was proposed by the European Commission on the 5th of February in 2019 that international negotiations should be commenced on cross-border access to electronic evidence in order to track down terrorists and dangerous criminals.[83] The purpose is to

[77] Fredman – Kanerva – Tolvanen – Viitanen 2020, p. 25.
[78] European Commission, SIRENE Cooperation. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation_en. Accessed 25.04.2023.
[79] *Ibid.*, p. 220.
[80] The Schengen Agreement, Sops 23/2001, Article 94(3)(f).
[81] *Ibid.*, Article 94(3)(a-c).
[82] *Ibid.*, Article 94(3)(g-h).
[83] https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en.

change the lengthier judicial cooperation procedures in terms of obtaining electronic evidence which poses a risk of having the sought data being moved or deleted. Procedures of voluntary cooperation with different service providers lack reliability, transparency, and accountability, and has a sense of legal uncertainty. E-evidence is supposed to give a possibility for authorities to circle these lengthy processes by providing national authorities a platform to obtain and request electronic evidence and data without interfering the affected person's rights.[84]

The Commission reached a provisional political agreement on 29th of November 2022 by the European Parliament and the Council on the new rules for sharing of electronic evidence in the EU.[85] In essence as first Vice-President Franc Timmermans stated, its goal is to prevent criminals, who may be benefitting from the exploitation of modern electronic communication technologies, from hiding their criminal actions and therefore evade from justice.[86] The modern electronic communication devices refer to text messages, emails and apps.

The proposals on the new E-evidence Regulation and the E-evidence Directive shall have some clearly envisioned purposes. First, it shall create a European Production Order which will give right to the judicial authority in one Member State to request emails, text messages etc. directly from a service provider providing services in the European Union which is established or represented in another Member State.[87] The location of data itself will not matter. The service provider will be obliged to respond to the request. This will surely aid in the crime investigations by making it more efficient. It will provide a better protection of the fundamental rights of the victim of crime and enable faster crime investigations. Before, the criminals have been able to often stay anonymous and therefore avoid being suspected of a crime, but also avoid from being recognized, found, arrested and therefore from being brought to trial and justice.

Secondly, it will give judicial authorities a right to oblige service providers located within

[84] European Commission: e-Evidence: Commission welcomes political agreement to strengthen cross-border access for criminal investigations 29.10.2022: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7246. Accessed 04.06.2023.
[85] *Ibid…*
[86] European Commission: Security Union: Commission facilitates access to electronic evidence: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343. Accessed 04.06.2023.
[87] *Ibid…*

the EU to preserve data so it can be requested by an authority on the basis of mutual legal assistance and European Investigation Order or European Production Order.[88]

One of the things the Commission is purporting to achieve with the E-evidence is to implement strong safeguards and remedies for data processing while widening the possibilities for authorities to process personal data and other different data categories. If the European Investigation Order would manifestly violate the fundamental rights of a person and therefore the Charter of Fundamental Rights of the European Union, the service providers, and persons whose data is being processed can request a review. The E-evidence also purports to provide additional requirements to obtain certain data categories.

For the purposes of gathering evidence in criminal proceedings, all service providers shall have one legal representative in the Union who will take care of the compliance and enforcement of decisions and orders which are issued by the competent authorities of the Member States for the purposes of crime investigation.[89] The legal representatives must be provided with the powers and resources that it takes to comply with decisions and orders sent by any Member State falling within the scope of the new Directive 2023/1544. Member States should ensure that the legal representatives residing in their territories truly have the necessary tools to comply.[90]

The service providers will not be able to explain their non-compliance on the grounds of ineffective internal procedures since now they are responsible and obliged to provide the necessary tools for their own legal representative. This applies similarly to any claims of legal representatives claiming that they do not have the powers to deliver the requested data.[91] This does impose a strict obligation to comply with the data requests of the national law enforcement entities. This creates a risk of ending up transferring data too extensively in the fear of violating the new additions in the legal framework of cross-border data transfers.

The new E-evidence Regulation and the Directive seem to be imposing more of an obligation for the service providers to provide the requested information to the law enforcement

[88] European Commission: Security Union: Commission facilitates access to electronic evidence: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343. Accessed 04.06.2023.
[89] *Ibid*…
[90] Directive (2023/1544), Recital 16.
[91] *Ibid*…

authorities opposed to the current situation where the requests have often been depending more on the willingness of the service provider to hand information down.

The Regulation on European Production Orders and European Preservations Orders[92] came into effect on 17.08.2023 and the Directive on laying down harmonized rules on the designation of designated establishment and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings also came into effect on the same day.[93]

It is stated in Recitals 6-10 of the Regulation[94] that as the network-based services do not require any physical infrastructure, the electronic evidence is generally stored outside of the investigating State or by a service provider established in another Member State. This causes gathering data for criminal investigations to be difficult. Another cause making the data gathering more difficult is the fact that the data transfer request is usually sent to the State which hosts multiple service providers and as the number of requests have multiplied in the recent decade the timeline to have your request answered has stretched quite lengthy. This of course leads to different deadlines being closed before the investigations have been finished and henceforth the criminals have been able to avoid facing the consequences for their crimes. It also makes multiple leads unavailable hence hindering the efficiency of crime prevention.

The application of the Regulation (2023/1543), according to Recital 21, shall not depend on the actual location of the service providers to encrypt data. This is because many of the service providers save data in cloud systems in which case the data has no physical location.

It is crucial that the service providers will under the E-evidence related legislative regime be obliged to provide the requested information within a certain time limit since it is part of the nature of the electronic evidence that it can be more easily and quickly deleted. Recital 15 recognizes that personal data obtained under the Regulation[95] must be processed when

[92] Regulation (2023/1543), p. 118–180.
[93] Directive (2023/1544).
[94] *Ibid.*, Recitals 6-10.
[95] Regulation (EU) (2023/1543), Recitals 15.

necessary for the purposes of prevention, investigation, detection and prosecution of crime or enforcement of criminal penalties and the exercise of the rights of defense.

One can criticize this to give extensive or at least very broad rights for the authorities to process personal data. Of course, for the safety of the EU nationals it is crucial that the malicious actors behind the different new platforms can be recognized, and different leads followed without bureaucratic dead ends caused by the current lengthy response times and the lack of information since part of it may have been for example deleted.

3. EXCHANGE OF DATA IN CRIMINAL PROCEEDINGS AS A REGULATORY TARGET

3.1. Principles relating to processing of personal data

For strengthening freedom, security, and justice in the European Union, the Hague Program was created in 2005.[96] *Gutiérrez* states that the Hague Program established a link between the principles of mutual recognition and mutual trust[97] and that they should be recognized in all steps of criminal proceedings[98]. After this a set of measures were taken to increase trust between the judicial authorities of the Member States.[99] Framework Decisions on confiscation,[100] financial penalties,[101] custodial sentences,[102] probation[103] and supervision measures[104] were adopted according to the Hague Action Plan. The most relevant legal instruments related to the principle of mutual recognition are the European Investigative Order (EIO)[105] and the European Freezing and Confiscation Order.[106] According to Recital 6 of the Directive[107] it was considered by the European Council in the Stockholm Program that setting up a comprehensive system based on the principle of mutual recognition should be pursued further in terms of obtaining evidence in cases with cross-border dimension. This is what the EIO was created for.

3.1.1. The principle of mutual recognition and mutual trust

The principle of mutual trust is stated in Article 2 of the Treaty on European Union (TEU).[108] In Council conclusions on mutual recognition in criminal matters it is described that 'the principle of mutual recognition is founded on mutual trust developed through the shared

[96] The Hague Programme 3.3.2005, p.1–14.
[97] Gutiérrez 2015, p. 425-453.
[98] Programme of Measures to implement the principle of mutual recognition of decisions in criminal matters. OJ C 12, 15.1.2002, p. 10.
[99] Gutiérrez 2015, p. 15.
[100] Council Framework Decision 2006/783/JHA, p. 59.
[101] Council Framework Decision 2005/214/JHA, p. 16.
[102] Council Framework Decision 2008/909/JHA, p. 27.
[103] *Ibid.*, p. 102.
[104] Council Framework Decision 2009/829/JHA, p. 20.
[105] Directive 2014/41/EU, L 130/1.
[106] Regulation (2018/1805) of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders. 28.11.2018, L 303/1 & Gutiérrez 2015, p. 16.
[107] Directive 2014/41/EU, L 130/1.
[108] The Treaty on European Union.Consolidated version 26.10.2012.

values of the Member States concerning respect for human dignity, freedom, democracy, equality, the rule of law and human rights'.[109] The purpose of this has been that the authorities could be with ease that other authorities are applying same standard of protection of rights in their criminal justice system. Of course, it is not an easy task to ensure that the Member States do in fact apply the same level of protection of rights in their criminal justice system. This is due to the prevailing legal, historical, cultural, and political backgrounds between the Member Stated.

The mutual trust principle can is established on many areas and through many layers within the EU. According to the latest SIRIUS Report, mutual trust is of importance to recognize challenges EU judicial practitioners are facing in this fast-growing field of data and development of technologies[110] and essential in creating bridges with different jurisdictions.

It can be said that mutual trust is presupposed in the principle of mutual recognition which has a close connection to fundamental rights and the concept of the rule of law.[111] It holds that judicial decisions made in one Member State should be accepted in the whole Union.[112]

Mutual recognition was developed in the context of single market (*Cassis de Dijon)*[113]. This of course means that should any Member State violate this; it consequently proposes risks for the trust in the EU and furthermore mutual recognition. The principle of mutual recognition also allows the judicial authorities to maintain direct contact which must happen in accordance with the principle of legality. The request depends on the importance of the committed criminal offence and must be drafted in accordance with the principle of proportionality.[114]

This principle has been mostly analyzed through the European Arrest Warrant (EAW)[115].[116] The EAW is a judicial decision issued by a Member State with a view to the arrest and

[109] Council conclusions on mutual recognition in criminal matters 'Promoting mutual recognition by enhancing mutual trust' (2018/C 449/02), p. C 499/6.
[110] Sirius EU Digital Evidence Situation Report 2022, p. 71.
[111] Bárd 2018, p. 1-2.
[112] *Ibid.*, p. 2.
[113] *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein,* Case C-120/78.
[114] Gutiérrez 2015, p. 159.
[115] Consolidated text: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).
[116] Valsamis 2009, p. 120.

surrender by another Member State of a requested person for the purposes of conducting a criminal prosecution or executing a custodial sentence or detention order.[117] The Warrant itself is a national judicial decision that must be executed by the requested State.[118] It must be implemented according to the Council of Europe Convention of 28 January 1981 and with regard to automatic processing of personal data, the personal data processed in this context should be protected according to the Convention.

EIO[119] provides law enforcement faster alternative framework for requesting evidence, compared to the traditional instruments. The investigative measures included are the hearing of witnesses, covert investigations, telephone interceptions and banking operation information.[120]

It is to be stated that the legality and proportionality principles should take preference always.

3.1.2. The principle of availability

The principle of availability of information is based on mutual recognition. The principle of availability concerns a presupposed agreement on what information is, how it should be handled, and how it can be used. It is presupposing that the 'organizational and cultural forms of different law enforcement entities are of sufficient proximity'.[121] This is to prevent the need for discussions of the power of each or on the distinction of information.

Gutiérrez is emphasizing on how the Hague Program recognized the details related to the cross-border exchange of information since it had a reference to the transfer of personal data for aviation security and to the principle of availability.[122] The Council from there on identified different aspects on access to information within the principle of availability which shall be presented below.

[117] Consolidated text: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA), Article 1(1).
[118] Valsamis 2009, p. 120-121.
[119] Directive 2014/41/EU, L 130/1.
[120] European Union Agency for Criminal Justice Cooperation, European Investigation Order: https://www.eurojust.europa.eu. Accessed on 10.05.2023.
[121] European Parliament Directorate-General Internal Policies Policy Unit C. Citizens' right and Constitutional affairs briefing paper: the Principle of Availability of Information, abstract.
[122] Gutiérrez 2015, p. 20.

Firstly, questions arose regarding the direct access of the requesting party to the data held in another Member State. Consequently, this came with several issues such as language differences between the Member States, information technology problems, and financial costs. There was either no ways to ensure that the principles and rights of data protection are followed accordingly.[123]

A second 'modality' was the information access upon a request – indirect access. Based on the principle of availability it seems, according to *Gutiérrez's* interpretation, it was the principle of equivalent access to available information that guided the Commission Proposal for a Council Decision on the exchange of information.[124] Again, there was a reluctance in the Member States as another similar simplifying and applicable initiative had been put forward called the Swedish Initiative[125].

Thirdly, there was an initiative that the European or national central index provided a way to indirectly reveal if there was any information on the person concerned available. This led to inspiring DNA search databases of the Treaty of Prüm[126] on a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. [127]

The strategy which was developed based on the principle of availability was the EU Information Management Strategy (IM).[128] Its purpose was to tackle the difficulties that arose from the proliferation of information systems, channels, tools, and legal instruments.[129] It is indeed of the most importance that the cross-border exchange of information is secure in order to achieve a steady internal security in the EU.

It shall be noted that even though the principle of availability is not expressly recognized in the Treaty of Lisbon[130], in Article 87(2)(a) it is stated that 'for the purposes of prevention,

[123] Gutiérrez 2015, p. 20–21.
[124] *Ibid.*, p. 21.
[125] Council Framework Decision 2006/960/JHA, p. 89–100 (The Swedish Initiative).
[126] Gutiérrez 2015, p. 21.
[127] *Ibid.*, p. 375-417.
[128] The EU Information Management Strategy, 5307/2/17 REV 2.
[129] Gutiérrez 2015, p. 30.
[130] The Treaty of Lisbon, OJ C 306,17.12.2007, p. 1-271.

detection and investigation of criminal offences, the European Parliament and the Council may establish measures concerning "the collection, storage, processing, analysis and exchange of relevant information"[131], echoing the principle of availability.

3.1.3. The principles of legality, proportionality, and purpose

Chapter 2 Article 4 of the LED (2016/680)[132], sets out the principles of legality, proportionality, and purpose which have already been established in the EU before. According to the Article, the Member States shall provide for personal data to be processed lawfully and fairly,[133] collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes[134]. Personal data must be accurate,[135] adequate, relevant, and not excessive in relation to the purposes for which they are processed.[136]

Data must be kept in such a manner that data subjects are protected from identification for no longer than is necessary for the purposes they are processed for.[137] Appropriate technical or organizational measures must be in place to ensures appropriate security of personal data.[138] These principles may be found from Article 4 of the Regulation 2018/1725 concerning Union entities.

All these aforementioned principles continue to have a relevant impact on processing and transferring personal data. They are cherished in most of the legislation concerning personal data.

[131] Gutiérrez 2015, p. 21.
[132] 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 OJ L119/89 4.5.2016
[133] Directive (2016/680), Article 4(1)(a).
[134] *Ibid.,* Article 4(1)(b).
[135] *Ibid.*, Article 4(1)(d).
[136] *Ibid.*, Article 4(1)(c).
[137] *Ibid.*, Article 4(1)(e).
[138] Directive (EU) 2016/680, Article 4(1)(f).

3.2. Fundamental Right to privacy and protection of personal data

3.2.1. European right to privacy and protection of personal data

The right to personal data protection was set in Article 8 of the Charter of Fundamental Rights of the European Union (CFR).[139] *Vogiatzoglou* and *Valcke* state that the European legal tradition is safeguarding a broader right to privacy which also protects individuals from unlawfully processing their own personal data.[140] Previous to, this the development of regulating data protection had been demonstrated in a plenty of national and international pursuits. Data protection was for example constitutionalized in the adoption of the Convention on the protection of individuals with regard to automatic processing of personal data by the Council of Europe (CoE).[141]

Article 8 of the European Convention on Human Rights (ECHR)[142] cherished the European right to privacy which was one of the first steps towards the right to data protection.[143] Article 8 of the Charter of Fundamental Rights of the EU gives emphasis that the protection of personal data is one of the fundamental rights of a person.[144]

According to Article 4(1) of the GDPR 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by a reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

---

[139] Charter of Fundamental Rights of the European Union [2016] (CFR). Art 8 CFR states: '(1) Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; (3) Compliance with these rules shall be subject to control by an independent authority.'

[140] Vogiatzoglou –Valcke in Research Handbook on EU Data Protection Law 2022 & European Convention on Human Rights [1950] (ECHR), Art 8; CFR, Art 7 & CFR, Art 8.

[141] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS No. 108 (Convention 108).

[142] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, November 1950, ETS 5.

[143] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 14.

[144] The Charter of Fundamental Rights of the EU, 2000/C 364/01.

As stated previously, there is an evident overlap between the fundamental rights of privacy and data protection stemming from the CFR but to what extent. According to *Vogiatzoglou and Valck* that right to personal data encompasses all information on the individual whether identified or identifiable no matter if it relates to private life or not. [145] The right to respect for private and family life concerns areas of private life that are irrelevant from data protection.

3.2.2. The hierarchy of 'personal data' provisions

Shall it be noted that it is a general practice of the EU law that secondary law should be interpreted in the light of primary law (*Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*[146] [2014]).[147] However, Vogiatzoglou and Valcke suggest that when it comes to interpreting Article 8 of the CFR, there are some leanings that invites to question whether it should follow the basic practices of EU interpretation.

Explanations of the CFR[148] lay down all the sources for its rights. It is to be noted that the fundamental right to personal data protection is drawn from the Directive 95/46/EC (DPD) provisions in secondary law.[149] Vogiatzoglou and Valck suggest that article 8 CFR could be interpreted in the light of the DPD[150] and the GDPR.

The cases[151] have shown a flexible interpretation according to which the CJEU interprets how primary and secondary provisions relationship should be approached. Article 8(2) of the CFR is referring to the principles of fairness, lawfulness and purpose specification and a right to rectification.[152] Article 8(1) and (3) of the CRF can be said to echo secondary law. Vogiatzoglou and Valcke have interpreted that Article 8(1) CFR is understood in a similar

[145] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 18.
[146] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], paragraph 68.
[147] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 20222022, p. 18 & Graig – de Búrca, 2020 ch 5. Instruments and the Hierarchy of Norms.
[148] Explanations relating to the Charter of Fundamental Rights [2007] & TEU, Article 6.
[149] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 19.
[150] Directive 95/46/EC, p. 0031 – 0050.
[151] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317.
[152] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 20.

broad manner as 'personal data' in the DPD. Vogiatzoglou and Valcke are hesitant of the fact whether the mentioned principles are bound by the second law rights or if they should be interpreted individually.[153] This hesitation comes from the fact that only certain principles and rights are included in the CFR provisions.[154]

The Court of Justice of the European Union (CJEU) has stated in *Google Spain SL and Google Ink v Española de Protección de Datos (AEPD) and Mario Costeja González*[155] that Article 8(2) and 8(3) should be interpreted alongside with Articles 6 (Data Quality Principles), 7 (Legal Grounds for Processing), 12 (The Right of Access), 14 (The Right to Object), and 28 (Supervisory Authority) of the DPD.[156]

The reason for why it is important to understand the impact of secondary legislation on the principles and rights in Article 8(2) CRF is because it aids in the process of understanding its limitations and therefore threshold for processing of data. Article 8(2) CFR and the part purpose specification requiring data to be 'processed fairly for specific purposes' is deemed as being too vague.[157]

What is not clear is if this represents secondary law purpose limitations as whole, including purpose and compatible use principles or solely the purpose specification.[158] If it was interpreted as including the compatible use principle it would need a table of interferences that can be done within the right to data protection.[159] *Vogiatzoglou and Valcke* state that it would be somewhat strange if secondary law provided broader level of protection than primary law. Advocate General Kokott in the case of *Productores de Música de España (Promusicae) v Telefónica de España SAU*[160] supported the view that Article 8(2) would enshrine the purpose limitation principle in light of the DPD.

[153] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 20.
[154] *Ibid…*
[155] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], para 69.
[156] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 20.
[157] *Ibid…*
[158] *Ibid…*
[159] *Ibid…*
[160] Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España* SAU [2008] ECR I-00271, Opinion of AG Kokott, para 53.

The CFE Explanations entail that secondary law contains conditions and limitations for the exercise of the right to the protection of personal data. The CJEU did not include the DPD provision on restrictions to Article 13 amongst those provisions by which Article 8(2) and (3) CFR are implemented. However, an examination by *Vogiatzoglou and Valcke* on the GDPR and the DPLED provisions which replaced the DPD, shows that it points to the CFR as a primary law regarding the assessment of the foreseen restriction test.

The GDPR Article 23 which is the successor of Article 13 of the DPD requires that necessity and proportionality laid in the CFR Article 52(1) must be met. It seems that those two hierarchically different legal provisions of primary and secondary law guide one another when one needs to assess the conditions and limitations. However, the starting point of assessment may be difficult to find because of this kind of 'circular approach'.[161]

Fuster has argued that the approach of the CJEU regarding Article 8 of the CFR seems to be downgrading it into a secondary law, although it is a fundamental right of data protection.[162] The suggested interpretation of article 8 'through the lens of secondary law'[163] fundamentally goes across with the EU primary law prevalence. It should be noted that the core of personal data is defined by secondary law and is thus not fully independent from it.[164] Thus, secondary law should be viewed as enshrining the fundamental right to data protection.

3.3. Other legislations regarding exchange of personal data in the context of criminal proceedings

3.3.1. International Agreements

There are multiple bilateral and multilateral state agreements in force between nations. Some of them require cooperation between authorities.

[161] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 21.
[162] González 2015 & Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 22.
[163] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 22.
[164] *Ibid…*

The Tampere programme

The Tampere Programme was created in a special meeting on 15 and 16 October 1999 in Tampere on the creation of an area of freedom, security and justice in the European Union. It was in the Tampere meeting when the European Council called the Council to provide Europol with support and resources. It recognized the need to strengthen its role in terms of receiving operational data from Member States.[165] The conclusions of the Tampere Council included goals to create and strengthen a common EU asylum and migration policy, a genuine European area of justice, a unionwide fight against crime and a stronger external action.

The Hague Programme

The objectives of the Hague Programme are found in Chapter 1 of the Hague Programme (2005/C 53/01). Its main goal, as stated before, is to enhance the common capability of the Union and 'guarantee fundamental rights…procedural safeguards and access to justice' for the Member States. One of the specified objectives is to fight cross-border crime and to realize the potential of Eurojust and Europol.

The suggestions to improve the exchange of information can be found in Chapter 2. It is stated that measures should hold up to the principle of availability. The framework requires that the authorities may exchange data if they are necessary in order for the legal tasks to be performed, the integrity of the data must be guaranteed, sources of information must be protected and confidentiality secured at all stages of the exchange of information, the data exchange must be supervised and controlled, and individuals must be protected from the abuse of data and be able to have information corrected. Data exchange should also make use of technology and central databases such as SIS.

The Prüm-Treaty

In 2006 Finland signed the Treaty of Prüm (Prüm, SopS 54/2007) and it came therefore into force 17.06.2007. The Prüm-Treaty has been ratified with law (277/2007)[166]. The law has

[165] Chapter IX of the Tampere European Council 15 and 16 October 1999 Presidency Conclusions.
[166] The Act on enhancing cross-border cooperation between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the Republic of Germany, the Grand Duchy of Luxembourg, the Kingdom

been since partly repealed by Law on enhancing cross-border cooperation between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria, in particular on the enactment of the provisions falling within the scope of the legislation of the agreement to combat terrorism, cross-border crime and illegal migration, and amending the law on the application of the agreements (1208/2011).[167]

Prüm is an implementation of the principle of availability which was introduced in the Hague Programme as a new approach to the cross-border data exchange between authorities.[168] The general data protection rules can be found in Chapter VII of the Prüm Treaty. The Treaty requires to follow the general principles of data protection in Articles 35-41 of necessity, legality, and purpose. In the center of Prüm was the development of exchange of DNA, fingerprint, and vehicle cross-border information.

Concerning the administrative and technical implementation and application of the Prüm Treaty, the Council adopted Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combatting terrorism and cross-border crime. Council Decision 2008/616/JHA was created on the implementation of Decision 2008/2015/JHA. The aim of these Decisions was to strengthen the cross-border data exchange of information and personal data in order for the EU law enforcement authorities to have access to all of the existing tools to combat crime and terrorism.

It is required in Article 5 of the Decision (2008/616/JHA) that the Member States take all necessary measures to ensure that comparison of DNA data, fingerprint data and vehicle registration can be conducted 24/7. The exchange of information must be confidential and

---

of the Netherlands, and the Republic of Austria, in particular on the enactment of provisions falling within the scope of the legislation of the Agreement on Combating Terrorism, Cross-Border Crime and Illegal Migration, and on the application of the Agreement (277/2007).

[167] The Act on enhancing cross-border cooperation between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, and the Republic of Austria, in particular on the enactment of provisions falling within the scope of the legislation of the Agreement on Combating Terrorism, Cross-Border Crime and Illegal Migration, and amending the Act on the Application of the Agreement (1208/2011).

[168] Opinion of the European Data Protection Supervisor on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (2007/C 169/02), paragraph, 3.

necessary steps must be taken to guarantee the integrity of DNA profiles (Article 7 of Council Decision (2008/616/JHA). Other Prüm Member States' authorities may access the DNA information through an automatic comparison of DNA in national contact points held by other countries (Article 3, 54/2007). This search can be done only in singular cases according to Article 3 subsection 1.[169] Another State's registered information visible to other contact points can only give out DNA-profile and a reference number. No personal data containing identifiable information shall be shared.[170] Only after a possible match of DNA, a detailed request can be sent to identify the person. NBI is the national contact point in Finland for DNA exchange.

According to Prüm it is possible for authorities to have a direct access to each other's vehicle registers in which case it is not possible to refuse the data request.[171] According to the Act on amending the law on transport services (301/2018) Chapter 3, 6 § the Department of Traffic Safety of Finland may share registered vehicle data for law enforcement tasks if the data sharing is based on law, EU law or international agreement. Hence, Prüm has enabled the automated exchange of data cross-borders between authorities.

European Commission gave a 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 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, and 2008/616/JHA on the implementation of Decision 2008/615/JHA.[172] The purpose of the proposal is to fill the gaps where data is stored in different national IT systems and on a EU level. It is explained in the section 'Reasons for the proposal' that there are 'blind spots' in the Schengen area without internal border controls for criminals and terrorists acting in more than one Member State.

It is notifiable that more than 70 % of organized crime groups are present in more than three Member States according to the proposal. In the proposal, what the Prüm-Treaty covered in terms of matching DNA, fingerprints and vehicle information is as terms are being expanded

[169] The Treaty of Prüm (54/2007).
[170] HE 243/2006, Yleisperustelut 4.1.
[171] *Ibid.*, Yleisperustelut 3.
[172] 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, Brussels, 8.12.2021, COM(2021) 784 final, 2021/0410(COD).

to cover other information such as face images, criminal records, and driver licenses. The purpose is to also connect all the data bases to each other with a central connector. Also, Europol shall be connected to the Prüm organization. The goal is to avoid having to use multiple channels to exchange data and at the same time enhance the integrity of the EU legal order.[173]

Council gave a recommendation based on the proposal[174] on 9 June 2022 on operational law enforcement cooperation.[175] It is to be noted that Recommendations do not have a binding force. Hence, the Member States may incorporate it to their national legislation according to the existing Union law.[176] Again, it is highlighted in Recital 8, that it is critical for a successful cross-border cooperation between law enforcement authorities to have a real-time access to the information kept in the Union systems. Authorities' mobile solutions, such as portable devices or in-car mounted law enforcement computers should provide this kind of access within the EU law framework.

Prüm II has been criticized by the European Digital Rights (EDRi) network. The EDRi published a position paper on 7 September 2022 which raised multiple issues with the proposal.[177] For example, it seems that the Proposal fails to take on the opportunity to fix certain systematic issues in the cross-border exchange by law enforcement entities under the current Prüm framework.

It is argued in the position paper that the Proposal does not sufficiently align with the Law Enforcement Directive (LED, 2016/680) which will be examined in detail later in this thesis. The proposal does not seem to argue the necessity and proportionality of its measures. Thus, it is posing a risk for the allowance of mass surveillance undermining the presumption of

[173] Savolainen 2022, Edilex toimitus.
[174] 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, Brussels, 8.12.2021, COM(2021) 784 final, 2021/0410(COD).
[175] Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation ST/8720/2022/INIT, *OJ L 158, 13.6.2022, p. 53–6.*
[176] *Ibid*., Ch. General Framework, pp. (a).
[177] European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022. Accessed 10.03.2022.

innocence.[178] Policy Advisor, *Jakubowska,* at EDRi has commented that if the Prüm Regulation proposal will not be improved extensively, it 'will be like pouring petrol on the fire that is the state of data collection, processing and cross-border exchange by law enforcement in Europe.'[179] Specifically the EDRi seems to be concerned that Member State nationals will be treated as if they are suspected of serious crimes and that the populations' fundamental rights will be breached by the inclusion of facial image exchange and by addition of the national driving license systems.

EDRi recommends that all searches should only be allowed in individual cases in the event of serious crimes and that the definition of 'police records' should be limited to ensure that for example biased assumptions would not be shared via Prüm II. Also, the proposal should have a thorough proportionality and necessity assessment to ensure a high level of protection of the fundamental rights related to privacy and data protection.[180]

The position paper sheds light on the difference in the level of protection of individuals residing in different Member States. The percentage of the population held in each national DNA database varies widely. It is problematic, when speaking on an EU level, that individuals registered in a police database in a Member State with lower threshold for inclusion have weaker safeguards. This will be more commonly led to unjustified police attention than individuals benefitting from higher standards. Thus, they will be under an enhanced risk of intrusions of their data protection rights.[181]

The Prüm II proposal seems to fail to recognize this particularity. For example, in Finland and Denmark the percentage of the population held in the national database is between 2 % and 5 %. In France this percentage is around 9 % and in contrast Portugal's DNA databases contain only 0.14% of their country's population. This calls upon an important question of

[178] European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022, p. 3. Accessed 10.03.2022.
[179] Wahl, Thomas, 'Civil Rights Organisations Criticise Prüm II Proposal'. Eucrim, 5 october 2022.
[180] European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022, p. 7. Accessed 10.03.2022.
[181] *Ibid.*, p. 8.

the necessity of a lot of profiles in the national databases.[182] This would essentially mean that 2-5% of Finland's population and 9% of France's would be suspected or convicted of serious crimes.

Another problematic issue that is reflected in the data which is collected and codified in different databases are some existing biases in the act of profiling related to race and ethnicity. This can enhance discrimination.[183] The discrimination is further exacerbated by the inclusion of inaccurate and poor-quality data in many European law enforcement databases.[184] In Slovenia, it has come to light that the victims and their family members have been included in criminal databases. Because of the lack of transparency of criminal databases and how data is processed, many do not know that their data is unlawfully processed and cannot therefore exercise their rights. Such breaches should not happen since including a person in criminal databases may have severe repercussions on their rights and liberties.[185] Malta, Austria and Romania had searched 99 % of their national DNA profiles in 2021 which calls into questioning whether each search did relate to a specific individual case and was in line with due process and the rule of law.[186]

The European Data Protection Supervisor (EDPS) issued EPDS Order to Europol to delete large datasets which had no established link to criminal activity.[187] In 2020 the Agency had systematic failings which led to large fundamental rights violations through data processing. Taking account these abuses, it is controversial for Prüm II to foresee Europol as the EU's criminal information hub with expanded powers as stated in Recital 3 of the Proposal.[188] The

[182] European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022, p. 8. Accessed 10.03.2022.
[183] *Ibid.*, p. 9.
[184] Dr. Toom, Victor June 2018, 'Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision: LIBE Committee Study': https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf. Accessed 20.03.2023.
[185] European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022, p. 10. Accessed 10.03.2022.
[186] *Ibid…*
[187] European Data Protection Supervisor, Annual Report 2022., p. 2. edps.europa.eu: https://edps.europa.eu/system/files/2023-04/23-04-26_edps_ar_2022_annualreport_en.pdf. Accessed 11.03.2023.
[188] European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed

EDRi is concerned that this will further aid in the broader rule of law crisis. It is explained in the position paper that 'we are witnessing the growing criminalization of political opposition, social movements, refugees and migrants…and investigative journalists' and criminalization of the ones aiding migrants for example in Hungary, Greece and Italy.

Now, the paper by the EDRi, is recommending that all countries and agencies participating in Prüm II should pass a full and independent *ex ante* data inspection before it is connected to the central router. The purpose of this would be to ensure that the data has been stored according to the law and according to the strict necessity and proportionality requirements of the LED which came into force after the original Prüm decisions. Another purpose is to ensure that officials are following the rules and procedures.

The goal is to set minimum requirements for what can be considered serious crime, ensure that victims or witnesses cannot be included, and standardize terminology from 'criminals' to 'persons convicted of a criminal offence'. Also, there should be a minimum requirement when a person's data should be removed from the database, i.e., persons who have been acquitted or charged should be removed. The paper is requiring all the connecting states to have national definition of 'reasonable suspicion' and requires that persons should be informed about their inclusion in the databases.

Prüm II should also require reports on the number of people contained in the databases and certain statistics and how guidelines on how it would be implemented under the LED. One important change the paper is suggesting is to delete the last sentence of Article 51.1 which states 'processing for other purposes…' since it allows Member States to process data via the Prüm framework but outside of its protections. It should be clarified that in accordance with the LED the processing of data must be strictly necessary, and the purpose must be explicit.[189]

Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022, p. 11. Accessed 10.03.2022.

[189] European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022, p. 12-13. Accessed 10.03.2022.

As seen there exists many issues in the Prüm II proposal which must be addressed in the following course to prevent further record of the abuse of data in policing databases such as Europol.

Napoli II

Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, so called Napoli II, was created to strengthen the commitments in the Convention on mutual assistance between customs administrations signed in Rome September 1967. The purpose of Napoli II was to strengthen the cooperation between customs authorities and Border Security. Title V governs data protection provisions. Article 25.1 requires that the customs administrations need to consider the specific data protection requirements upon each case. The recipient authority may then forward the data to its customs administrations, investigative authorities, and its judicial bodies (Article 25.2(a)). Subsection c of the article highlights that when data should according to the law be erased or amended, the person that it concerns needs to have a right to correct that data, the exchanged data must be recorder and it should not be kept longer than what is necessary for the purposes they were communicated (g).

3.3.2. Finnish Legislation

The first data protection law in Finland that came into force was the Personal Data Act (471/1987).[190] It was later, after Finland joined the EU 1995, repealed by the Personal Data Act (523/1999). It implemented the Personal Data Directive 95/46/EY which is now repealed by the GDPR. Data Protection as a fundamental right has been in the Constitution of Finland (731/1999) since 1995. Chapter 2, Section 10 of the Constitution of Finland states that everyone's private life is guaranteed.

The Data Protection Act (1050/2018) fulfils the GDPR nationally. The LED has been implemented into the national legislation by the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018). The GDPR and the LED shall be discussed in detail later in section 3.5.

[190] Kurvinen 2021, p. 80.

Finland has special legislation concerning data processing concerning prevention of crime.

Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018) implements the EU's Data Protection Directive for Police and Criminal Justice Authorities with regard 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, and on the free movement of such data.

When it comes to the police's statutory duties, the Act on the Processing of Personal Data by the Police (616/2019) takes precedence. In 2021 the Ministry of Interior requested opinions on the implementation of the 2019 new Act. According to those opinions, the objective of this legislation is to ensure that the police is able to react fast to the changes in the security environment. Another objective is to secure the flow of correct information that is necessary to the activities of the Finnish authorities and to secure the processing of personal data in crime prevention.[191]

The Act on the Processing of Personal Data by the Police (616/2019) considers all of the above data sharing platforms which the law enforcement in Finland is using explained in Chapter 2. The police may process personal data almost whenever it is deemed necessary to do so. As the police is the authority signing permits, it has wider rights to process personal data for other duties than crime prevention as well. The NBI, the Finnish Security and Intelligence Service and Customs have the central access points referred to in Article 3 for obtaining information from the VISA System to prevent, detect and investigate certain offences listed in Section 18 of the Act.

Section 25[192] governs the disclosure of personal data to law enforcement authorities of a Member State of the European Union or of the European Economic Area according to which the police may disclose information to competent authorities of another Member State of the

[191] Ministry of the Interior: Effectiveness of the new Act on the Processing of Personal Data by the Police to be assessed. 22.04.2021: https://intermin.fi/en/-/effectiveness-of-the-new-act-on-the-processing-of-personal-data-by-the-police-to-be-assessed. Accessed 02.04.2023.
[192] The Act on the Processing of Personal Data by the Police (616/2019).

European Union who processes the data for the purposes in the LED (article 1(1)). The police may also disclose information on personal data to Eurojust and other established agencies under the TFEU which is responsible for safeguarding legal and social order but also maintaining public order and security[193]. According to Section 27 of the Act[194], the police may disclose information from multiple systems. Section 30 implements the Prüm decision to apply to the disclosure of DNA. The Act[195] refers also to the application of the Framework Decision (26/2009)[196] which was created to simplify the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

The Act on the Processing of Personal Data by the Police is a special law that was drafted to complement the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (490/2023) but also the GDPR and the Finnish Data Protection Act.

As the protection of national security has been declared to be protected by the national authorities in Article 2(2) of the TEU, the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (490/2023) governs the transfer of data linked to national security in safeguarding against, and preventing threats to, public security in connection with activities related to preventing, detecting or investigating criminal offences or referring them for consideration of charges, and other activities of a prosecutor in relation to criminal offence, hearing a criminal case in court and enforcing a criminal sanction.[197]

In terms of protecting national security, the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (490/2023) applies, according to Chapter 1 Section 1, to the processing of personal data by and on behalf of the Defence Forces and Defence Command. It is to be noted that the Act only applies if the

[193] Treaty on the Functioning of the European Union, C326/49.
[194] The Act on the Processing of Personal Data by the Police (616/2019).
[195] *Ibid.*, Section 26.
[196] Council Framework Decision 2006/960/JHA.
[197] Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (490/2023), Chapter 1, Section 1.

processing of personal data is wholly or partly automated or if the data to be processed form or are intended to form a filing system or a part of it. The Act implements the LED.

The Act on the Processing of Personal Data by the Customs (650/2019) governs the data processing in the tasks assigned to the Customs for the purposes of preventing, detecting or investigating criminal offences or referring them for consideration of charges, consideration of charges and other activities of a prosecutor in relation to criminal offence according to Section 1 of the Act. The data processing must be done according to the fundamental rights and data protection principles. According to Section 20 the Customs may transfer bulks of personal information to the police, Border Security, Military, prosecutors, and courts referred to in the Data Protection Act (1050/2018).

The customs may transfer personal data listed in Sections 7-10 of the Act on the Processing of Personal Data by the Customs (650/2019). The personal data listed in these Sections relates to the parties in a case including the victim and the witnesses, images, biometric information, and other information related to the identification of a person related to a crime.

The provisions related to the Finnish Border Guard relates to the processes to prevent breaches of provisions on crossing the national or external border, according to Section 5 of the Act on the Processing of Personal Data by the Border Guard (639/2019). As law enforcements entities generally, the Border Guard also has substantial rights to process personal data for the purposes of investigating offences and maintaining public order and security.

The Act on Cooperation between the Police, Customs, and the Border Guard (687/2009) was created to strengthen the national cooperation between the police, customs and the Border Guard. The goal was to strengthen the cooperation in such a manner that it would be more appropriate, efficient, and cost-effective. In general, the authority who gets information on a crime, must inform the authority to whose function it belongs to (Section 2).

3.3.3. European Legal Norms

Article 8 of the European Convention on Human Rights (ECHR)[198] cherished the European right to privacy which was one of the first steps towards the right to data protection.[199] There was a need to harmonize and promote the free flow of personal data within Europe for which Convention 108 and Protocols[200] from the Council of Europe (CoE) was adopted.[201] It was the first binding international instrument that aimed to protect an individual from possible abuse caused by collection and processing of personal data and regulated the trans frontier flow of personal data.

The convention also safeguards an individual's right to know that their information is stored and a possibility to have it corrected. It also prohibits the processing of sensitive data such as criminal record and health in the absence of proper legal safeguards. It also imposed restrictions of cross-border dataflow of personal data where the other country does not provide equivalent protection.[202] This is what linked data protection to human rights and data protection became recognized as a term internationally in Europe.[203]

Bygrave presents that this is when technologically expanded surveillance and control capabilities began to 'disempower the individual' around 1960's, risks to privacy became identified.[204]

In 1992, in the Treaty of Maastricht[205] it was held that serious forms of international crime were of the common interest of the EU. It introduced the three-pillar structure which consisted of European Community (first pillar), the common foreign and security policy (CFSP) (second pillar) and cooperation in the fields of justice and home affairs (third pillar). Cross-border exchange of information was not frequent among the authorities located in different Member States yet.[206] In the third pillar laid out in the Treaty of Maastricht

[198] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, November 1950, ETS 5.
[199] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 14.
[200] ETS No. 108, 01/10/1985 (5 Ratifications.).
[201] Council of Europe on Details of Treaty No. 108: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Accessed 17.05.2023.
[202] *Ibid…*
[203] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 15.
[204] Bygrave 2002. See, Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 13.
[205] The Treaty of Maastricht, 07.02.1992.
[206] Gutierréz 2015, p. 18.

framework decisions were made. They were directive-like in the first pillar as they had to be implemented in the national legislation in a form and method in which Member States chose to achieve the objectives of those decisions.[207] Framework decisions established objectives which Member States were expected to fulfil. They however did not have a direct effect on Member States although they were binding on the Member States.[208] Direct effect is an EU law doctrine that allows individuals to invoke an EU law provision before a national court.[209] Thus, individuals could not have invoked framework decisions before domestic courts.[210]

It shall be noted that although the framework decisions are not recognized by the Treaty of Lisbon and were replaced by Directives, the existing ones have been preserved until amendment or annulment. For example, framework Decision 2008/977/JHA and Council Framework Decision 2006/960/JHA which the LED repealed is currently still in force. They concern simplifying the exchange of information and intelligence between law enforcement authorities of the Member States[211]. Cross-border exchange of information was not frequent among the authorities located in different Member States yet.[212] *Gutierréz* has stated that terrorist attacks which took in place in New York and Washington in 2001 resulted in the European Arrest Warrant (EAW). It was adopted at the JHA Council meeting in June 2002 and accelerated the process to develop cooperation.[213]

The Data Protection Directive (DPD)[214] was the first EU legislation on data protection.[215] Its purpose, as interpreted by *Vogiatzoglou and Valke*, was to improve the free flow of personal data and to protect fundamental rights and freedoms of natural persons specifically their right to privacy upon data processing.[216]

In the early 2000's Regulation on the protection of individuals regarding the processing of personal data by the Community institutions and bodies and on the free movement of such

[207] EUmonitor.eu: framework decision.
[208] Brewczyńska 2022 in Research Handbook on EU Data Protection Law 2022, p. 98 reflecting on Case C-105/03 *Criminal Proceedings against Maria Pupino* [2005] ECR I-5285.
[209] *Van Gen den Loos v Netherlands Inland Revenue Administration.* 07/03/1985 European Court Reports 1985 -00779 ECLI identifier: ECLI:EU:C:1985:104.
[210] Mitsilegas 2009, p. 26
[211] Council Framework Decision 2006/960/JHA.
[212] Gutierréz 2015, p. 18.
[213] *Ibid.*, p. 14.
[214] Directive 95/46/EC.
[215] Vogiatzoglou – Valcke in Research Handbook on EU Data Protection Law 2022, p. 16.
[216] *Ibid…* & Directive 95/46/EC (DPD), Article 1.

data[217] was established. It was stated that a first step in the area of data protection on the protection of personal data is the Convention on the Use of Information Technology for Customs Purposes and the Schengen Convention to develop fundamental principles in the fields of judicial cooperation in criminal proceedings and police and customs.[218]

A year later Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) was created. It recognized the risks internet poses to its users.[219] Regulation (2018/1725) on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of such data was created and it continued to link data protection and privacy repealing Regulation (EC) No 45/2001.

The Treaty of Lisbon[220] can be said to have been the first legislative measure to lay the foundation for the intra-EU cooperation concerning Criminal Justice. [221] It had a great impact on the development of the data protection legal framework but also on the area of freedom, security and justice (AFSJ) in the European Union.[222] It can be said to have made AFSJ one of the main political priorities for the EU.[223] The Treaty of Lisbon also demolished the EU 'pillar structure' and one of its purposes was to align the EU criminal law rules regulating the police and judicial cooperation in criminal matters.[224] As an aftermath of the entry of force of Lisbon, data protection has been enshrined in Article 8 of the Charter of Fundamental Rights (CFR)[225].

The DPD was repealed by the EU reform package which included the Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data,

[217] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1.
[218] *Ibid.*, Recital 17.
[219] Directive 2002/58/EC (e-Privacy Directive), Recital 6.
[220] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007); entry into force on 1 December 2009, p. 1-271.
[221] Sirius EU Digital Evidence Situation Report 2022, p. 5, 26, 37 & 73.
[222] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 94.
[223] *Ibid…*
[224] *Ibid…* See Mitsilegas, p. 37.
[225] Charter of Fundamental Rights of the European Union OJ C 326 26.10.2012.

repealing Directive 95/46/EC and Directive (EU) 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 (DPLED)[226]. Now, almost every new EU legislation starts by stating personal data protection as a fundamental right[227] under the Charter of Fundamental Rights (CFR)[228] related to the Treaty on European Union (TEU) Article 6 which states that fundamental rights shall constitute general principles of the Union's law[229].

The main difference between the Data Protection Directive and the Framework Decision was that the Framework Decision had a quite limited scope of application. The latter did not govern situations related to domestic processing. This led to criticism and created doubt in terms of relevance of the Framework Decision and its role in strengthening the right to the protection of personal data in the field of criminal law.[230]

As stated, Council Framework Decision 2006/960/JHA is still in force, and it has been implemented into Finland's legislation by law (26/2009)[231]. This Decision is purported to ease the data exchange between national authorities in order to complete a criminal investigation.[232] An authority is obliged to send personal data to the requesting authority in another State if it is necessary for the purposes of a criminal investigation.[233]

The definition of personal data referred in 3 § can be found in the Act on the processing of personal data in police work (761/2003) 2 §. Personal data that can be requested consists of information relating to police's working security, basic information, search warrants, different restraining orders, arrests, criminal history, reports of investigations, DNA

[226] Directive (EU) 2016/680.
[227] GDPR, Recital 1; DPLED, Recital 1; Regulation (EU) 2018/1725, Recital 1.
[228] Charter of Fundamental Rights [2007] OJ C303/02.
[229] TEU OJ C 326, 26.10.2012, p. 13–390, Article 6.
[230] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 98. See e.g., EDPS, 'Opinion on the Communication from the Commission on 'A Comprehensive Approach on Personal Data Protection in the European Union'' 14.01.2011, para 129
[231] Act on the national implementation and application of the provisions of the Framework Decision of the Council on simplifying the exchange of information and intelligence between the law enforcement authorities of the member states of the European Union (26/2009).
[232] Council Framework Decision 2006/960/JHA, Recital 7.
[233] Act on the national implementation and application of the provisions of the Framework Decision of the Council on simplifying the exchange of information and intelligence between the law enforcement authorities of the member states of the European Union (26/2009), 5 §.

information, images etc (2:1-11 §). According to 7 § an official must refuse from the cross-border exchange of data when it may endanger Finnish national security[234], if the request conflicts with fundamental rights[235], it would be against the fundamental principles of the Finnish Legal order to provide information,[236] and if sending information needs a permission from a judicial authority.[237] An official may also refuse a request if it takes unnecessary attention, fulfilling the request may harm the investigation in Finland or the crime under investigation is not such that could be examined as a crime for which a maximum penalty in Finland would be more than one year of imprisonment.

3.4. Comparative assessment of the GDPR and the LED

The two main secondary law legal instruments of the EU data protection framework are the GDPR, 2016/679[238] and the LED, 2016/679[239]. Although both instruments were adopted based on Article 16 of the Treaty on the functioning of the EU (TFEU)[240] which states that everyone has the right to the protection of personal data concerning them[241] and form a part of the so-called data reform package[242], these two provisions still constitute two separate legal provisions and have different thresholds for the protection of personal data.[243] These two provisions continue to keep data processing for law enforcement purposes separate from the general data processing operations.[244]

[234]Act on the national implementation and application of the provisions of the Framework Decision of the Council on simplifying the exchange of information and intelligence between the law enforcement authorities of the member states of the European Union (26/2009), 7 § subsection 1.
[235] *Ibid.,* 7 § subsection 2.
[236] *Ibid.,* 7 § subsection 3.
[237] *Ibid.,* 7 § subsection 4.
[238] 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) OJ L119/1 4.5.2016 (GDPR).
[239] 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 OJ L119/89 4.5.2016 (LED).
[240] Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012.
[241] *Ibid.*, Article 16(1).
[242] European Commission - Fact Sheet Questions and Answers - Data protection reform package**,** What about the Data Protection Directive for the police and criminal justice sector? http://europa.eu/rapid/press-release_MEMO -17-1441_en.htm. Accessed 01.04.2023.
[243] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 91
[244] Lynskey 2019, p. 162.

The European Commission has stated on their fact sheet regarding the data protection reform package that the purpose of the LED is to protect personal data of individuals having a part in criminal proceedings and to facilitate 'a smoother exchange of information between Member States' police and judicial authorities'.[245] The main goal can be said to be ensuring a high level of protection of personal data whilst taking into account the special nature of police and criminal justice field.[246] Another one is to contribute to the ASFJ.[247] This is accordingly with the primary EU law which provides that the free movement of persons should be guaranteed in order to guarantee the functioning of the internal market along with the provision of appropriate measures for combatting and preventing crime.[248]

Chapter 2 Article 10 of the GDPR governs processing of personal data relating to criminal convictions and offences. It states that processing of personal data relating to criminal convictions and offences, or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of an official authority.

Article 6 of the GDPR states that the processing shall be lawful if one of the following applies to the situation at hand: the data subject has given consent to the processing of his or her personal data for one or more specific purposes,[249] 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,[250] processing is necessary for compliance with a legal obligation to which the controller is subject,[251] processing is necessary in order to protect the vital interests of the data subject or of another natural

[245] European Commission - Fact Sheet Questions and Answers - Data protection reform package**,** What about the Data Protection Directive for the police and criminal justice sector? http://europa.eu/rapid/press-release_MEMO -17-1441_en.htm. Accessed 01.04.2023. See Directive (EU) 2016/680.
[246] LED, Recital 11.
[247] European Commission - Fact Sheet Questions and Answers - Data protection reform package, What about the Data Protection Directive for the police and criminal justice sector? http://europa.eu/rapid/press-release_MEMO -17-1441_en.htm accessed 1 April 2021). See Recital 2 LED.
[248] Article 3(2) Consolidated version of the Treaty on European Union OJ C 326 26.10.2012. Article 67(1) TFEU. See. Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 92.
[249] GDPR, Article 6(1).
[250] *Ibid.,* Article 6(2).
[251] *Ibid.*, Article 6(3).

person,[252] 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,[253] 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.[254]

The question to be asked therefore is, what are the delimitations between the LED and the GDPR?

3.4.1. The scope of the application of GDPR and the impact of the e-Privacy Directive

The GDPR applies to all processing of data and to all its citizens.[255] The Regulation can be said to have changed the perception of the importance of individual's data privacy in the EU.[256] The GDPR essentially governs data sharing, processing, and usage.

The material scope of the regulation is defined in Article 2. Article 2(1) states that the Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. *Brewczyńska* has interpreted this provision to mean that the GDPR governs automated processing and manual processing.[257]

According to Article 4(7) a 'natural or legal person, public authority, agency or other body' carries out the data processing either as a data controller or data processor. According to *Lynskey* the purpose to name such a variety of different entities with either public or private legal status sheds light that the intention of the legislator was not to have the level of data protection be dependent on whether it is a public or private entity that controls the data processing.[258]

[252] *Ibid.*, Article 6(4).
[253] *Ibid.*, Article 6(5).
[254] *Ibid*, Article 6(6).
[255] *Ibid,*, Article 1. See: Sharma – Menon 2020 1st edition, p. 45.
[256] Sharma – Menon 2020 1st edition, p. 45.
[257] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 99.
[258] Lynskey 2016, p. 16.

It should be considered that although as a Regulation, the GDPR has a direct effect in the EU, in order to adapt to the obligations, some national legislation needs to be adapted. This of course poses a risk that the Member States may eventually have differences in the level of protection of personal data across the EU caused by the divergences in the implementation of the GDPR.[259]

Principle of subsidiarity provides a template for debate concerning the scope of application of the Regulation. According to this principle, EU can practice legislative intervention only when the Member States cannot sufficiently achieve the proposed action.[260] However, having an EU regime which applies to all different legal entities processing personal data is convincing, given the inherent cross-border character of data flows.[261] This is the reasoning the European Commission used to justify the necessity to establish EU rules concerning the processing of personal data although there is a risk of divergencies and restrictions on cross-border flows of personal data between the Member States.[262]

Brewczyńska argues that it is beneficial for the EU citizens that there exists the same level of data protection in every Member State through comprehensive rules.[263] This would not be possible without the EU legislative intervention. What justifies having both public and private legal entities covered in the regime is the fact that the GDPR has been adopted on the basis on Article 16 TFEU which opened a broader mandate for the EU to legislate and set safeguards to protect the fundamental right to the protection of personal data. EU legal framework in this area is justified as the GDPR has not been adopted on the basis concerning internal market and Article 114 TFEU.[264]

[259] EDRi, Proceed with Caution: Flexibilities in the General Data Protection Regulation' (5.7.2016) https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf accessed 15.3.23 & Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 100.
[260] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 100.
[261] *Ibid*...
[262] *Ibid*...
[263] *Ibid*...
[264] *Ibid*...

An activity falling outside the scope of EU law

Firstly, Article 2(2)(a) shall be examined regarding data processing in the course of an activity which falls outside the scope of Union law. According to Recital 16 of the GDPR, this provision does not apply to activities that concern national and common security.

National security as a notion can be argued being ambiguous and there are significant problems arising from its definition and scope since it very much depends on international and European law but also on the national policies of the Member States.[265]

It has been traditional for the EU not to mandate in the area of national security because it has been seen as an element of the State sovereignty with which Article 4(2) TEU correlates with by stating that 'national security remains the sole responsibility of each Member State'.[266] Article 73 TFEU echoes the previous and highlights that it is to the Member States to organize the coordination between the entities in charge of their national security.

However, this does not explicitly mean that the questions regarding or having links to national security of a Member State would render it automatically outside the scope of application of the EU regulatory framework. Furthermore, it would exempt a Member State from the obligation to comply with the fundamental rights regarded by that EU framework.[267] It was stated by the CJEU in the case of *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*[268] when relied on other preliminary rulings[269] that although it is the role of a Member State to define their essential security interests and to adopt the necessary measures, this practice cannot render the EU law inapplicable and exempt a Member State from its obligation to comply with EU law.

[265] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 101.
[266] *Ibid…*
[267] *Ibid…*
[268] *Privacy International* [6 October 2020], paragraph 44.
[269] Judgments of 4 June 2013, *ZZ*, C-300/11, EU:C:2013:363, paragraph 38 and the case-law cited; of 20 March 2018, *Commission* v *Austria (State printing office)*, C-187/16, EU:C:2018:194, paragraphs 75 and 76; and of 2 April 2020, *Commission* v *Poland, Hungary and Czech Republic (Temporary mechanism for the relocation of applicants for international protection)*, C-715/17, C-718/17 and C-719/17, EU:C:2020:257, paragraphs 143 and 170).

Brewczyńska has led from the conclusion of the court in *Privacy International*[270] that the Court held in a nutshell that although a Member State has declared national security as its purpose, this should not lead to the reduction of the scope of the EU legal framework.[271] An assessment should be always conducted on a case-by-case basis when determining if the EU law is applicable. The CJEU seems to also imply that EU law can be restricted only partially where for the other part there is room to interpret exceptions to attain to the goals of protecting national security.[272]

Article 15 of the e-Privacy Directive[273] states that the Member States may restrict the scope of rights and obligations by adopting different legislative measures when it is necessary, appropriate, and proportionate to safeguard State security.[274] In GDPR a similar provision can be found in Article 23.[275]

In *Privacy International* the Court clarified that the e-Privacy Directive governs all data processing regardless of the receiver of data.[276] Thus, when intelligence services request data for the purposes of national security that falls under the e-Privacy Directive[277] also.[278] In *Privacy* International it became relevant that the previous should not be affected by derogations from the application the e-Privacy Directive providing that the Directive should not apply to any activities falling outside of the scope of the EU law. It does not neither apply to activities concerning public security, defense, State security and the activities related to criminal law.[279]

The e-Privacy Directive seems to grant the Member States authorization to adopt national legislative measures if the certain conditions are met. Therefore, Article 15(1) can be said to presuppose that the national legislative measures to fall within that scope.[280] The activities

[270] *Privacy International* [6 October 2020].
[271] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 102.
[272] *Ibid…*
[273] Directive 2002/58/EC (Directive on privacy and electronic communications).
[274] *Ibid…*
[275] 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.
[276] *Privacy International* [6 October 2020], paragraph 36.
[277] *Ibid…*
[278] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 102.
[279] *Ibid…*
[280] *Ibid.*, p. 103.

that are deviated and fall outside the scope of EU law according to Article 1(3) of the e-Privacy Directive are not 'exclude a priori applicability of the data processing rules established under this legal act (GDPR)'.[281]

Conclusion:

It has been seen that the GDPR and e-Privacy Directive both exclude from the scope of its application processing of personal data when it relates to an activity which falls outside of the scope of EU law.[282] Recital 16 of the GDPR clarifies that the previous relates to national security by stating that Article 2(2)(a) is not applicable to national security. However, according to Article 23 of the GDPR safeguarding national security can justify restrictions imposed on the obligations and rights established under the GDPR.

When comparing Articles 1(3) and 15(1) of the e-Privacy Directive and Articles 2(2)(a) and 23(1)(a) GDPR, it seems that some of the processing of data when carried out in the context of national security could still need to comply with the GDPR and its requirements, but also interpreted in the light of the CFR.[283] *Brewczyńska* sheds light on this with an example where 'the personal data is initially collected by entities to whom and for the purposes to which the GDPR applies and is then further processed 'in the course of an activity which falls outside the scope of EU law'.[284] In this case an intelligence agency receiving transmission of data from an entity governed by the GDPR will fall under the scope of GDPR. Processing of data in the context of national after the transmission of data can be said to fall outside of the scope of the GDPR.[285]

Exception regarding law enforcement

Article 2(2)(d) states that the GDPR[286] does not apply to 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, including the

[281] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p.103.
[282] *Ibid…*
[283] Brewczyńska, p. 103. See: Kranenborg, Herke, 'Commentary on Article 2 Material Scope' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds) The EU General Data Protection Regulation: A Commentary (OUP 2020), 69.
[284] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 103.
[285] *Ibid…*
[286] Regulation (EU) (2016/679), p. 1–88.

safeguarding against and the prevention of threats to public security. *Brewczyńska* specifies that the application of the previous exception depends on the personal and material criteria being fulfilled together.[287] The range of data controllers is namely limited to the ones stated in Article 2(2)(d). Recital 19 states the following: 'This Regulation should not, therefore, apply to processing activities for those purposes.' When a processing attempts to reach the goal of a law enforcement, it does not bring the activity outside the scope of the GDPR automatically. However, if an activity is not carried by a competent authority according to the LED, the processing for law enforcement purposes does fall under the GDPR stated in Article 23(1)(d).[288]

A list of conditions under which processing can be restricted is stated in Article 23 GDPR. The restriction must serve one of the goals laid in Article 2(2)(d) and national security. The restriction should be a legislative measure and respect the 'the essence of the fundamental rights and freedoms and [be] a necessary and proportionate measure in a demo- cratic society' according to Article 23 GDPR. GDPR does not only authorize Member States to adopt necessary measures which restricts rights and obligations but specifies conditions when it is possible to do so. Brewczyńska concludes that the GDPR applies in the context of activities of law enforcement, justifying the restrictions.[289]

In terms of the material scope of the GDPR, it is dependent on the purpose of the processing. The law enforcement purposes that lay outside of the scope which are prevention, investi- gation, detection or prosecution of criminal offences or the execution of criminal penalties.

In conclusion it seems that the processing with fall outside the scope of application of the GDPR must satisfy personal and material criteria. The formulation of this criteria in Article 2(2)(d) of the GDPR is overlapping the manner in which the scope of application in the LED is stated in Article 1(1) and Article 2(2).[290]

[287] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 103.
[288] *Ibid…*
[289] *Ibid…*
[290] *Ibid.,* p. 104–105.

3.4.2. The scope of the application of LED

Ensuring security and justice are one of the values EU has seeked to enforce since the Treaty of Lisbon[291] came into force with respect for fundamental rights[292]. It is to be noted that the LED[293] was adopted based on Article 16 of the TFEU[294] which states that everyone has the right to the protection of personal data. This provides for a consistent and high level of protection of personal data. Many other instruments in the field of EU criminal law are based on Article 83 of the TFEU[295] enabling judicial or police cooperation.

Brewczyńska is concerned that shaping the rules of activities carried out in judicial cooperation in criminal matters is difficult as they should correspond to its nature and objectives.[296] It is however of a great importance to do so. According to the European Data Protection Supervisor (EDPS), the processing of personal data must be limited to the areas where specific rules are truly necessary.[297]

'A Competent Authority'

The requirement of competent authority[298] being the one to carry out the processing refers to the personal scope of application of the LED.[299] 'Competent authority' according to Article 3 indent 7 of the LED means any public authority which is competent 'for the 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 or any other body or entity entrusted by Member State law to exercise public

[291] Document 12007L/TXT, Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, *OJ C 306, 17.12.2007, p. 1–271 (BG, ES, CS, DA, DE, ET, EL, EN, F*
[292] Article 67(1) TFEU.
[293] 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 OJ L119/89 4.5.2016.
[294] Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, p. 47–390.
[295] *Ibid…*
[296] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 105.
[297] EDPS, 'Opinion 6/2015 A Further Step towards Comprehensive EU Data Protection. EDPS Recommendations on the Directive for Data Protection in the Police and Justice Sectors' (2015), 5-6.
[298] Article 2(1) LED.
[299] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 106.

authority and public powers for the purposes of the 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'. Thus, a competent authority refers to law enforcement authority and other bodies and entities that have been assigned with law enforcement tasks by the national law.

This notion of a 'competent authority' in the context of data protection means data controller. According to Article 3 indent 8 of the LED ''controller' means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.

As a result of the Treaty of Lisbon the EU has competence to lay down rules that must be limited, according to Article 82(2) TFEU, 'to the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension.'

It is to be noted that when the LED was drafted it could not be foreseen that there would be a need to update a list of competent authorities for the purposes of the LED under national laws. 'Such obligation exists, for instance, under the Council Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States.[84] Having a publicly available centralised EU registry of competent authorities would clarify the doubts related to the scope of Article 3 indent 7(b) of the LED and make the provision much easier to implement.[300]

'For the purposes of the 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' sets out the purpose of the processing of personal data (Article 1(1) LED). All of the mentioned purposes, except the execution of criminal penalties, refer to 'criminal offence'. However, what constitutes as a criminal offence is not defined in the LED. Recital 13 only states that it is an autonomous concept of EU law as

[300] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 108.

interpreted by the CJEU. This poses a risk of having too wide interpretation of what constitutes a criminal offence. Criminal offence is generally defined in national laws making it a term dependent on each legal system of each Member State.

The doctrine of autonomous concepts seems to have become an important tool in terms of managing national diversity and reinforcing the effectiveness of the EU law.[301] What makes this area of harmonization of EU somewhat difficult is that the area of criminal law is rooted in the State's characteristics and traditions.[302] *Brewczyńska* has come to the conclusion that it causes confusion that Recital 13 LED explicitly states the concept of criminal offence to be autonomous and cannot be endorsed by the Member States as a useful tool to figure out the framework of the LED.

It is to be noted that the CJEU is built upon the jurisprudence of the European Court of Human Rights (ECtHR).[303]Landmark case of handling the jurisprudence of the CJEU was the case of *Engel and Others v. the Netherlands*[304] which established the Engel criteria[305]. In the case of *Bonda* the Engel criterion was interpreted that firstly, it must be examined what is the legal classification of the offence under national law. Secondly, it must be examined what is the nature of the offence and thirdly, what is the nature and degree of severity of the penalty that the person concerned is liable to incur.[306] In *Engel* the ECtHR had to examine whether an offence in the case at hand was criminal or disciplinary and if the applicants could exercise their right to a fair trial stipulated in Article 6 ECHR.

In Commission Expert Group meeting on 7th of November 2016 the *Engel* criteria was supported as it has been accepted by the case law of the CJEU.[307] However, in Commission Expert Group discussions on 4th of May 2017 it was contended by the European Commission's Legal Service that when interpreting the LED, Member States can rely on the

[301] *Ibid.*, p. 109. See: Valsamis Mitsilegas, 'Autonomous Concepts, Diversity Management and Mutual Trust in Europe's Area of Criminal Justice' (2020) 57(1) *Common Market Law Review* 45, 45.
[302] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 109.
[303] *Ibid…*
[304] *Engel and Others v. the Netherlands* (1976) Series A no 22.
[305]*Bonda* [2012] Case C- 489/10, ECLI:EU:C:2012:319 para. 37. See: *Sergey Zolotukhin v. Russia*, no. 14939/03, §§ 52 and 53, 10 February 2009).
[306] *Bonda* [2012] Case C- 489/10, ECLI:EU:C:2012:319 para. 37.
[307] Commission Expert Group, Minutes of the meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (7 November 2016) para 1.

notion of criminal offence defined in their national laws.[308] This was stated to end the discussion where certain processing of personal data in administrative proceedings or misdemeanors should be considered falling under the LED in Member States where these proceedings are distinct from crimes.[309]

This can be seen as giving a way an EU-wide criteria for the definition of a criminal offence in terms of the harmonization of the data processing rules of the EU. Another danger exists which is that that LED's interpretation expanded by its application since the Member States can determine what constitutes as a criminal offence, where there will be no need to consider the general rights guaranteed by the GDPR.[310]

Prevention, investigation, detection and prosecution of crime and execution of penalties:

The purpose of an investigation is to find evidence and a suspect which will lead to a confirmation of them committing or not committing a crime.[311] Prosecution refers to the moment when the prosecutor files a court charge against the suspect for the alleged crime. What finishes the trial stage is the execution of criminal penalties. The actual court procedure seems to be outside of the scope of the LED but according to Recital 20, the LED does not exclude Member States from specifying data processing procedures in court proceedings.

It is evident that the law enforcement activities differ from state to state. The LED does not provide details on the scope of different activities for the purposes of the EU law. This can be argued to leave quite a large amount or room for the Member States to define the exact scope of application of the LED. Thus, national law should define what falls under definition of criminal offence, what are the limitations on investigation, detection or prosecution and execution of penalty and what fulfils the material scope of application of the LED.[312]

[308] Commission Expert Group, *Minutes of the meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680* (4 May 2017), para 1.
[309] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 110.
[310] *Ibid…*
[311] *Ibid…*
[312] *Ibid…*

Threats to public Security:

The phrase added by the Council[313]: 'including the safeguarding against and the prevention of threats to public security' as a formulation of the purposes of data processing in law enforcement context and as a definition of a competent authority shall be addressed next.

The phrase can be seen as another attempt to provide a wider leeway for the member states to regulate from the narrow 'role and objective of criminal law and the needs of criminal proceedings that can justify application of the specific data protection regime'[314] expanding the meaning of the law enforcement tasks under the LED. LED's material and personal scope of application refer to the phrase' safeguarding against and the prevention of threats to public security'.[315]

In LED Recital 12 extends this in the way that the relevant activities undertaken by the police or other law-enforcement authorities can cover 'maintaining law and order as a task conferred on the police or other law-enforcement authorities where it is necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence'.[316] This can be said to waive the LED slightly further again from 'criminal offence' as a notion as it stretches the interest to 'fundamental interests' of the society. Again, this has been criticized by the Article 29 Working Party of having a risk to extending material and personal scope of the LED to a wider range of entities whose activities are only partly related to the purposes of the LED.[317] Using the notion of 'the prevention of threats to public security' is not linked to the concept of criminal offence.[318]

[313] Position (EU) No 5/2016 of the Council.
[314] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 112.
[315] *Ibid…*
[316] *Ibid…*
[317] Article 29 Working Party, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' (1 December 2015) WP233,
[318] Brewczyńska, Magdalena, A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation in Research Handbook on EU Data Protection Law. Edward Elgar Publishing 2022, p. 112.

Summarizing the findings of the LED

As seen, there are some visible differences in the data protection legal framework in the field of criminal law between the Member States.

LED and GDPR provide the objectives and the material scope of their application in the first two articles of each legislative regime. The GDPR does not include the specific processing operations included in LED.[319] LED is limited 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, including the safeguarding against and the prevention of threats to public security'.[320] This does not belong within the scope of GDPR.[321] Seemingly, it can be stated that when the rules of the LED apply, the rules of the GDPR do not.

The minutes of the Commission Expert Group meetings on the GDPR and the LED show that there is uncertainty from the Member States on how these legal provisions should be applied next to each other as there is a possibility of certain non-law enforcement entities falling from a gap either under the GDPR or the LED depending on the entity.[322] This is because LED's scope reaches beyond the police and criminal justice to certain private entities. An example of these are security service contractors.[323] According to the minutes from the expert group revealed that drawing delimitations between these two provisions is difficult as investigating misdemeanors as a branch of criminal law, may belong to entities that are not part of law enforcement. Hence, having to interpret the LED.[324] Thus, the provisions are not fully exclusive from one another. The processing of data by actors (FIUs: Financial Intelligence Units) in the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) can fall under either provision – GDPR or LED – depending on the type of processing and the entity itself.

[319] Brewczyńska 2022, p. 92.
[320] Article 1(1) LED.
[321] Brewczyńska 2022, p. 92.
[322] *Ibid*...
[323] Caruana 2019, p. 252.
[324] Commission Expert Group, Minutes of the meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (7 November 2016) para 1.

Brewczyńskska casts light on the unclear delimitations between the LED and the GDPR and the fact that the ambiguous nature of the LED could damage the legal certainty of the data protection legal framework.[325] This brings the question regarding the scope of rights available to data subjects and controls imposed on data controllers 'depending on the applicable regime'.[326] This would further invite the questions on whether different bodies should cooperate to enable the application of both legal provision on certain data processing matters.[327]

One of the main questions of competence has been how much room is there for the Member States to legislate in the area of protection of personal data since the EU legislator acted on the basis of Article 16 TFEU when adopting the GDPR and LED.[328] *Hijmans* has interpreted that there is not much room when taken into consideration the scope and nature of the mandate of the EU legislator under Article 16(2) TFEU.[329] *Hijmans* interpretation seems to fit with the GDPR regime as it covers multiple policy areas under the competence of the EU where processing of personal data can take place.[330]

It should also be noted that the GDPR is a regulation which means it is binding in its entirety and directly applicable in all Member States leaving barely any room for discretion.[331] LED however is a directive and is therefore binding to the result it wants to achieve. This can be achieved according to the methods the Member State wants to apply.[332] According to *Brewczyńska*'s interpretation, an obstacle in terms of harmonization of the rules for the processing of personal data in the law enforcement context arises from the LED's proximity to the criminal justice process which is chraracterized by the different regimes of each Member State.[333]

It should be noted that any conferred competence shall be always governed by two other fundamental principles of EU law: the principle of subsidiarity and proportionality.[334]

[325] Brewczyńska 2022, p. 93.
[326] *Ibid…*
[327] *Ibid...*
[328] Brewczyńska 2022, p. 96.
[329] Hijmans 2016, p. 268.
[330] Brewczyńska 2022, p. 96.
[331] Article 288 TFEU.
[332] Brewczyńska 2022, p. 96.
[333] *Ibid…*
[334] *Ibid…*

According to Article 5(3) of the Treaty on European Union (TEU) the principle of subsidiarity states that all of the EU-level actions should be implemented only when necessary and when it is better achieved on a Union level that national level. This principle differentiates from the principle of proportionality in such a way that the latter demands the EU action to be appropriate and necessary but not excessively in order to achieve the goal.[335]

The LED was created to govern the processing of personal data by the competent law enforcement authorities for law enforcement purposes. To trigger the application of this regime personal and material scope set out in Article 2(1) LED must be fulfilled. Whoever is not competent must handle the processing of data under the general regime.

On the level of secondary law, the GDPR and the LED seem to have fairly clear borderlines. The problems that are present arises from the wide room for maneuver provided by the LED in terms of determining the entities that fall under the LED as a competent authority and the activities in terms of the processing purposes referred to in Article 1(1) LED. Hence, all the differences between the Member States such as legal traditions may lead in different assessments of when the conditions are fulfilled for the application of LED.[336]

3.4.3. Conclusions on the delimitations between the GDPR and the LED

The minutes of the Commission Expert Group meetings on GDPR and LED shows that there is uncertainty from the Member States on how these legal provisions should be applied next to each other as there is a hesitancy of certain non-law enforcement entities falling from a gap either under the GDPR or the LED depending on the entity.[337] This is because the LED's scope reaches beyond the police and criminal justice to certain private entities. An example of these are security service contractors.[338] According to the minutes from the expert group revealed that drawing delimitations between these two provisions is difficult as investigating misdemeanors as a branch of criminal law, may belong to entities that are not part of law

[335] Hijmans 2016, p. 137.
[336] Brewczyńska 2022, p. 114.
[337] Brewczyńska 2022, p. 93.
[338] See Caruana, Mireille, 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2019) 33(3) Int Rev Law Comput Tech 249, 252. See Brewczyńska 2022, p. 93.

enforcement. Hence, having to interpret the LED.[339] Thus, the provisions are not fully exclusive from one another. The processing of data by actors (FIUs: Financial Intelligence Units) in the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) can fall under either provision – GDPR or LED – depending on the type of it.

It has been seen that the GDPR and e-Privacy Directive both exclude from the scope of its application of the processing an activity which falls outside of the scope of EU law.[340] Recital 16 GDPR clarifies that the previous relates to national security by stating that Article 2(2)(a) is not applicable to national security. However, according to Article 23 of the GDPR safeguarding national security can justice restrictions imposed on the obligations and rights established under the GDPR.

The LED and the GDPR provide the objectives and the material scope of their application in the first two articles of each legislative regime. The GDPR does not include the specific processing operations included in the LED.[341] The LED is limited to the processing of personal data 'by com- petent authorities for the purposes of the 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'.[342] This does not belong within the scope of GDPR.[343] Seemingly, it can be stated that when the rules of the LED apply, the rules of the GDPR do not.

Brewczyńskska casts light on the unclear delimitations between LED and GDPR and the fact that the ambiguous nature of LED could damage the legal certainty of the data protection legal framework.[344] This could enforce the question regarding the scope of right available to data subjects and controls imposed of data controllers 'depending on the applicable regime'.[345] This would further invite the questions on whether different bodies should cooperate.[346]

[339] Brewczyńska 2022, p. 92. See Commission Expert Group, Minutes of the meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (7 November 2016) para 1.
[340] Brewczyńska 2022, p. 103.
[341] *Ibid.*, p. 92.
[342] LED Article 1(1).
[343] Brewczyńska 2022, p. 92.
[344] *Ibid.*, p. 93.
[345] *Ibid…*
[346] *Ibid…*

One of the main questions of competence has been how much room is there for the Member States to legislate in the area of protection of personal data since the EU legislator acted on the basis of Article 16 TFEU when adopting the GDPR and LED.[347] *Hijmans* has interpreted that the is not much room given consideration of the scope and nature of the mandate of the EU legislator under Article 16(2) TFEU.[348] This interpretation seems suitable for GDPR since it covers many policy areas where processing of personal data can take place.[349] It should also be noted that the GDPR is a regulation which means it is binding in its entirety and directly applicable in all Member States leaving barely any room for discretion.[350] LED however is a directive and is therefore binding to the result it wants to achieve. This can be achieved according to the methods the Member State wants to apply.[351] According to Brewczyńska's interpretation, an obstacle in terms of harmonization of the rules for the processing of personal data in the law enforcement context arises from the LED's proximity to the criminal justice process which is chraracterized by the different regimes of each Member State.[352]

The development of harmonized data protection legal regime which is based on the principle of mutual recognition instead of EU integration poses multiple challenges. These are resulting from the legal, political, and cultural traditional differences of the states and constitutional backgrounds.[353]

As stated, any conferred competence should always be governed by the principles of subsidiarity and proportionality.[354]

The LED was created to govern the processing of personal data by the competent law enforcement authorities for law enforcement purposes. To trigger the application of this regime personal and material scope set out in Article 2(1) LED must be fulfilled. Whoever is not competent must handle the processing of data under the general regime. *Brewczyńska* has come to the conclusion that member states can entrust data controllers with the relevant

[347] Brewczyńska 2022, p. 96.
[348] Hijmans 2016, p. 268.
[349] Brewczyńska 2022, p. 96.
[350] Article 288 TFEU. See Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 96.
[351] Brewczyńska 2022, p. 96.
[352] *Ibid…*
[353] *Ibid,,,*
[354] *Ibid…*

public powers and authority and hence have the processing covered by the LED. Or Member States can legislate and restrict the scope of relevant rights and obligations of the general data protections regime in line with Article 23 GDPR.[355]

It can be said that on the level of secondary law, the GDPR and the LED seem to have clear borderlines. The problems that are present arises from the wide room to maneuver provided by the LED in terms of determining the entities that fall under the LED as a competent authority and the activities for processing purposes referred to in Article 1(1) LED. Hence, all the differences between the Member States such as legal traditions may lead in different assessments of when the conditions are fulfilled for the application of LED.[356]

It is evident that LED fails to consider the problems cause by diversity in national legal, cultural, and political traditions. By adding the phrase 'safeguarding against and prevention of threats to public security', the legislator has allowed Member States to restrict the fundamental right to data protection further.

[355] Brewczyńska 2022, p. 113.
[356] *Ibid.,* p. 114.

4. CONCLUSIONS

4.1. Challenges regarding protection of personal data in criminal matters

The continuously developing regime of data protection legal framework seems to in its current state to be posing multiple challenges. The goal of the European Union is to harmonize the data protection rules in which it is making progress. Lately this has been through the data protection reform package consisting of the GDPR and the LED and furthermore the E-evidence. Yet, at the same time there exists scholarly opinions about these legal provisions being broadly expanded to govern multiple entities outside of law enforcement by having the notions of a 'competent authority' and 'criminal offence' too broadly determined or not determined at all and left to the Member States to define. It is claimed that this is making interpretation of the two provisions confusing.

Some factors that cause challenges to the EU integration process are resulting from the legal, political, cultural, and traditional differences of the states and their different constitutional backgrounds.[357]

In some of the Member States biases in the profiling systems based on race and ethnicity are evident, enabling possible discrimination.[358]

4.1.1. Unlawful processing of personal data in criminal matters

Many European law enforcement databases are consisting of weak quality of data which is often also incorrect.[359] As a result, victims and their family members have been included in criminal databases and therefore have had their personal data processed unlawfully. Since these persons do not know that their data is being processed on criminal grounds, they cannot request it to be corrected. This is because of the lack of transparency in the processes of collection of

[357] Brewczyńska 2022, p. 96.
[358] European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022, p. 9.
[359] Dr. Victor Toom, June 2018, 'Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision: LIBE Committee Study':
https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf.

personal data. Large-scale problems arise from having one's personal data included in criminal databases as it can have unwanted and unlawful consequences. As a response to this issue, The European Data Protection Supervisor (EDPS) issued EPDS Order to Europol which simply ordered the Europol to delete bulks of data that is not linked to criminal activities. [360]

The aforementioned is one reason why it is difficult for Prüm to view Europol as the EU's criminal information hub with extensive powers. The nature of the type of abuses explained above may lead to the criminalization of the people who should not be criminalized.

The European Parliament in 2022 opened an investigation into the NSO Group. Their Pegasus spyware was used for unlawful state hacking against politicians, human rights defenders etc. One fear related to the application of the Prüm Treaty has been that it may exacerbate the criminal treatment of migrants and asylum seekers. This would for obvious reasons be outside of its purpose of tackling serious crime. This would indeed further contradict international humanitarian obligations.[361] *Taylor* has highlighted that there is a growing assumption that having one's personal data processed is a part of the contemporary social contract and therefor the processing of one's data should be justified.[362]

It has been suggested by the EDRi that the countries participating in the Prüm II should go through a data inspection which should be completed independently before connecting it to the main router. This would serve multiple purposes. Firstly, it would aid in ensuring that country has stored the data according to the law but also according to the principles of necessity and proportionality stemming from the LED as requirements. Secondly, the compliance of the officials in terms of the rules and procedural conduct must be checked.

4.1.2. The existing unclarities regarding the lack of thorough determination of notions

As declared in this thesis, there exists some criticism that may hamper the integrity of the EU wide crime investigations between the Member States or at least pose concerning questions

[360] European Data Protection Supervisor, Annual Report 2022: edps.europa.eu: https://edps.europa.eu/system/files/2023-04/23-04-26_edps_ar_2022_annual-report_en.pdf. p.2.
[361] European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation (Prüm II). 7 September 2022, p. 12.
[362] Taylor 2017, s. 1.

regarding it. These relate to the attempt of the EU to harmonize the rules for data processing in the context of law enforcement. As stated in Recital 13 of the LED there may be a need to have the notion of 'criminal offence' determined autonomously in the EU as there seems to be unclarity on the determination of a criminal offence. The unclarity upon the mentioned notion may give data processing rights on matters which are only on the limit of being determined as a criminal offence since there is a lack of clear guidelines.

The other matter which poses questions and makes the current data protection legislation risky, is that the LED lists multiple activities that belong to the law enforcement. These activities may bring data processing under the application of the LED but the LED fails to recognize the differences in the characteristics between the organizations of the Member States. It also seems that one of the problems of the LED is the fact that the legislator has allowed contradictions between the Member States by adding to the law enforcement purposes crime prevention and to be quoted 'safeguarding against and prevention of threats to public security'.

It is difficult to scrutinize whether the LED could have been built and worded in such a manner that it would have had served the purpose of harmonization of the EU better or its scope of application drafter in a way that there would not have had been as wide applicability for data processing of variety of entities.

Hence, it seems that the Member States have a right to restrict the fundamental right to data protection further in cross-border data transfers by the law enforcement and competent authorities since the wording of the phrase 'safeguarding against and prevention of threats to public security' under the LED.

Crime prevention has been defined by *Welsh* and *Farrington* as referring to efforts to prevent crime or criminal offending in the first instance – before the act has been committed.[363] Strategies in crime prevention have been debated with regards to data protection. For example, predictive policing technologies[364] are concerning from the view of data protection.

[363] Welsh – Farrington 2012, p.3.
[364] Lynskey 2019, p. 162.

4.1.3. Difficulties imposed on the protection of personal data by predictive policing technologies

Predictive policing technologies according to *Lynskey* are precarious and to be doubted.[365] Predictive policing refers to 'any policing strategy or tactic that develops and uses information and advances analysis to inform forward-thinking crime prevention'.[366] Automated decision making is one example of a predictive policing technology. In some digital services the harvesting of personal data is the prerequisite in getting an access to the service.

The danger is that these technologies will bring innocent people to conduct. The data protection and substantive prohibition on automated decision making has caveats through which it is possible to bypass them. The GDPR and the LED will be governing these automated policing technologies and specifically the LED in the context of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties. However, it is yet unknown whether the processing of personal data for these purposes falls within the scope of data protection.[367]

Another danger, according to *Welsh* and *Farrington* is that although the specific data protection rules such as limited transparency in covert operations can be viewed as justifiable, there is a risk that a too wide range of police activities will fall under the term of crime preventions. If prevention takes place 'outside of the confines of the formal justice system', it is possible to go over the LED and the requirements of proportionality and necessity.[368]

Brewczyńska is hesitant of the inclusion of the purpose of crime preventions may have more discrepancies hampering the objective of harmonization of data protection rules in the law enforcement context.[369]

When it comes to the accessibility of data and specifically personal data in the different modern electronic communication services, a threat of having one's data breached and accessed without

[365] *Ibid…*
[366] Uchida CD A National Discussion on Predictive Policing: Defining our Terms and Mapping Successful Implementation Strategies, California. (2009) NCJ 230404.
[367] Lynskey 2019, p. 163.
[368] Welsh – Farrington 2012, p. 3.
[369] Brewczyńska in Research Handbook on EU Data Protection Law 2022, p. 112.

a proper checking of the necessity requirement 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 exists. Hence, there seems to be a risk of possibly having non-suspects or non-criminal's data personal data processed during a criminal investigation without a reason.

4.1.4. Reflecting on the new legislation regarding E-evidence

Carrera, Stefan and Valsamis stated in 2020 that there should be a mechanism to evaluate EU mutual recognition instruments in criminal matters in order to enhance transparency.[370] They are suggesting that there should be a single EU portal of communication and transmission of European Investigation Orders between the judicial authorities to have a secured and trusted communication platform.[371] It seems that this quest has gotten an answer in the form of the E-evidence.

The new E-evidence related Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceeding and for the execution of custodial sentences following criminal proceedings states that for the purposes of maintaining an area of freedom, security and justice, the Union shall be adopting measures related to the judicial cooperation in criminal matters and based on the principle of mutual recognition of judgments and judicial decisions which have been the cornerstone of judicial cornerstone of cooperation in criminal matters within the Union since the Tampere conclusions.[372]

The new E-evidence proposals do guarantee that national's data shall be protected in due course. However, the wider the access to these serves and the information it holds within, the wider the rights to process person's data without one knowing their data is being processes. Therefore, arguably E-evidence poses another risk of giving the law enforcement authorities very wide access to personal data without any secure legal thresholds which again conflicts with the fundamental principles of having one's data processed only as far it is proportionate and necessary.

[370] Carrera etc 2020, p. 69.
[371] Carrera etc 2020, p. 70.
[372] Regulation (EU) 2023/1543, Recital 1.

The E-evidence regulates in a manner in which the location of the data will not matter. On a positive note, it shall on the other hand fasten the processing of data by posing an obligation on the service provider to send the requested data within a set time limit. The service provider will be obliged to respond in 10 days and in a case of emergency within 6 hours. It will provide a much better change to follow leads compared to the existing time limit of 120 days for the EIO or 10 months for Mutual Legal Assistance Procedure.

The new E-evidence has taken into account the nature of data which is that the electronic evidence can be deleted easily and fast. This is also why there are multiple benefits to the obligation imposed on service providers to provide the requested information within a certain time limit.

Again, it is stated in Recital 15 of the Regulation 2023/1543 that personal data requested and therefore transferred under the Regulation must be done in due process of prevention, investigation, detection and prosecution of crime or enforcement of criminal penalties and the exercise of the right of defense. This must be done by ways of respecting the fundamental principles of proportionality and necessity. Criticism has stemmed from the interpretation of the LED regarding the new E-evidence related Regulation 2023/1543 which is that the sentencing in Recital 15 may become in practice a veil for a very broad right to process personal data.

The E-evidence related Regulation does in Recital 14 state that Member States do need to ensure that the personal data are protected and still processed in accordance with Regulation 2016/679 and Directive 2016/630 and Directive 2002/58/EC meaning that the narrower definition of a competent authority under the existing legal framework will apply. According to the Regulation, only authorized persons should have access to information containing personal data which can be obtained through an authentication process.[373] The efficiency of the safeguards such as authenticator systems shall be seen in due course when the legislation comes into force.

As the network-based services can be provided from any location and do not require a physical infrastructure in the country where the service is actually provided in or in the internal market,

[373] *Ibid.*, Recital 15.

it can be hard to enforce any obligations to provide data for law enforcement by an order (EIO) or a decision by a judicial authority. The Directive 2023/1544 laying down harmonized rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings related to E-evidence recognizes the presence of this issue when the service is provided from a location outside of that Member State's jurisdiction.[374]

The Directive 2023/1544 attempts to facilitate a more effective criminal law enforcement in the Union and the area of freedom, security and justice by encouraging to prevent future divergent national approaches and existing obstacles to the free provisions of services should be removed and legal representatives appointed.[375] The legal representatives of relevant service providers shall be working as addressees for decisions and orders. This will be for the purposes of gathering electronic evidence based on Regulation 2023/1543.[376]

4.2. Future for the processing of personal data in the criminal law context

It seems that some of the protection offered by the data protection framework is more illusionary. There has clearly been a lack of clarity in terms of the existing legal framework which has created a risk in the absence of an EU wide approach, in terms of obtaining electronic evidence including personal data, which allows the Member States to impose different national obligations.

4.2.1. Legal uncertainties

This kind of enforcement and effective application of the Member States' own legislation can be said to create obstacles to 'the free provision of services within the internal market'.[377] This kind of divergences create legal uncertainty not only service providers but for national authorities. Conflicting national obligations on service providers established or functioning in many Member States, as they usually are, may be subjected to a variety of penalties in cases of

[374] Directive 2023/1544, Recital 1.
[375] *Ibid.,* Recital 5.
[376] *Ibid.*, Recital 6.
[377] *Ibid…*

violations. These differences in the legal framework considering criminal proceedings are in a danger of expansion as the importance of the information society services grows.[378]

This is specifically in the context of processing of personal data in the functions on predictive policing technologies. Article 2(2)(d) of the GDPR excludes from its scope data processing by competent authorities for the 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. The LED however does apply to this directly. As seen however, the GDPR is yet not fully excluded from the application even in the context of law enforcement. The delimitations between the GDPR and the LED were examined in Chapter 3.5.

In order to fall within the scope of the LED, the data processing must be undertaken by a 'competent authority'. If there is no legislative enactment for an entity being a 'competent authority', the provisions under the GDPR will continue to apply even to private entities who are processing personal data for law enforcement purposes.[379] This is confirmed by Article 23 of the GDPR. Even though the processing would be undertaken by a competent authority, the processing may fall under either the LED or the GDPR depending on its purpose. Data transfers for example from police to predictive policing software is covered by the LED where data is transferred from a competent authority to a non-competent authority because the processing of personal data is for law enforcement purposes and a data transfer non-law enforcement purpose such as a transfer to medical services is covered by the GDPR.[380]

As seen, neither of the provisions apply for example to the processing of personal data for the purposes of national security.[381] Although the LED states '…including the safeguarding against and prevention of security threats' as a purpose for a competent authority to process data it does not according to *Lynskey* provide any clearance on the existing blurred distinction between law enforcement activity, national security and public security.[382] Although, national security should be amongst the essential functions of a state according to Article 4(2) TEU, it seems to remain according to the same provision, as 'the sole responsibility of each Member State'.[383]

[378] Directive 2023/1544, Recital 3.
[379] Lynskey 2019, p. 165.
[380] *Ibid*...
[381] Directive 2016/680 (LED), Article 2(3) and Recital 14.
[382] Lynskey 2019, p. 165.
[383] *Ibid*...

It has been unclear whether predictive policing technologies shall be governed by the data protection law as being considered as personal data since it seems to require that the individual should be identifiable.[384] *Taylor* has highlighted that as the predictive policing technologies often profile and inform about actions of a group, it will be necessary to look beyond the individual level.[385]

According to the data protection laws, personal data means any information relating directly or indirectly to an identified or an identifiable natural person. In *Breyer*[386], it was held that when a website owner whose site would be under a cyber-attack could liaise with the authorities with identify information such as the internet service provider and therefore data could be linked to an identifiable person. This of course poses a risk of having the data protection law regulating a bit of everything[387] and many forms of data 'irrespective of their proximity to the data subject'.[388]

Evidently, whenever data will be collected for the projects in these new technology platforms it may be classified as personal data.[389] *Purtova* is suggesting that perhaps the distinction between personal and non-personal data should be abandoned and to bring the processing of all data under protection.[390] As the predictive policing technologies are to gain more developments, it is to be seen how the current unclear application of data protection rules shall be developed. The application of the new E-evidence and the impact it will have on the harmonization and effectiveness on the processing of personal data in the law enforcement context shall be seen in the following years. As *Taylor* has stated, it will be necessary to determine the ethical path in the datafying world in terms of data justice and fairness regarding the way people are 'made visible, represented and treated as a result of their production of digital data'.[391]

[384] Lynskey 2019, p. 165.
[385] Taylor 2017, p. 8.
[386] *Breyer v Bundesrepublik Deutschland*, Case C-582/14, pp. 23–24.
[387] Lynskey 2019, p. 172.
[388] *Ibid…*
[389] Purtova 2018, [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355]. Accessed 15.07.2023.
[390] *Ibid…*
[391] Taylor 2017, p.1.