STUDY

Requested by the LIBE Committee

European Parliament

Assessment of the implementation of the Law Enforcement Directive

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 740.209 - December 2022

EN

Assessment of the implementation of the Law Enforcement Directive

Abstract

This study analyses the main provisions of the Law Enforcement Directive as well as their implementation within national laws. In that context, the study identifies shortcomings and explores potential ways forward through a concrete set of recommendations.

This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Civil Liberties, Justice and Home Affairs.

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

AUTHORS
Plixavra VOGIATZOGLOU, KU Leuven Faculty of Law & Criminology – Centre for IT & IP Law – imec
Thomas MARQUENIE, KU Leuven Faculty of Law & Criminology – Centre for IT & IP Law – imec

Under the academic supervision of: Prof Dr. Peggy VALCKE, KU Leuven Faculty of Law & Criminology – Centre for IT & IP Law – imec

With the assistance of: Donatella CASABURO, Ezgi EREN and Flavia GIGLIO, KU Leuven Faculty of Law & Criminology – Centre for IT & IP Law - imec

ADMINISTRATOR RESPONSIBLE
Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT
Ivona KLECAN

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in November 2022

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

CONTENTS

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
AG	Advocate General
AI	Artificial Intelligence
AML	Anti-Money Laundering
CEG	Commission Exert Group
CFD	Council Framework Decision 2008/977/JHA
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECSPs	Electronic Communications Service Providers
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EPD	E-Privacy Directive – Directive 2002/58/EC, as revised
EPPO	European Public Prosecutor's Office
EU	European Union
EUDPR	European Union Data Protection Regulation – Regulation (EU) 2018/1725
FIUs	Financial Information Units
GDPR	General Data Protection Regulation – Regulation (EU) 2016/679
LED	Law Enforcement Directive – Directive (EU) 2016/680
PNR	Passenger Name Records

TFEU	Treaty on the Functioning of the European Union
WP29	Article 29 Working Party

EXECUTIVE SUMMARY

The Law Enforcement Directive (LED) was adopted in order to provide for high standards of data protection and support the free flow of data in the law enforcement and criminal justice sector. However, it should not be forgotten that the LED constitutes an instrument of minimum harmonisation; it must be transposed into national laws and it often affords broad discretion to Member States, risking divergent implementations.

This study **analyses the LED framework and its implementation** amongst Member States **as discussed by available sources**. It seeks to **identify shortcomings** and **explore potential ways forward**. A preliminary version of the study was submitted in February 2022 in order to inform the European Parliament in relation to the evaluation and review of the Directive which was due by the European Commission by 6 May 2022. The final version of the study has been further updated on the basis of the report by the European Commission on the Implementation of the Directive, as well as on the basis of latest legal developments. With a **regrettable delay of more than two months**, the European Commission published its first report on application and functioning of the LED on 25 July 2022. It consists of a brief document prepared on the basis of a variety of sources from EU institutions, national supervisory authorities and civil society organisations.

Under Articles 1 and 2, both the material and the personal scope of the LED are defined by virtue of terms that further rely on national legal orders, such as criminal offence, prosecution and execution of criminal offences, public security and competent authority. Reports have shown that Member States follow **divergent approaches** before and after the adoption of the LED. Such lack of harmonisation results in **legal uncertainty**.

More specifically, albeit autonomous, currently there is **no concrete EU-wide definition of what constitutes a criminal offense**. The concept of public security may be subject to both broad and narrow interpretations, while national security remains a concept in flux and equally vague, despite recent case law. As a result of the divergent national interpretations of the notions of public and national security, **the application of the LED rules through national law risks being expanded or limited beyond its intended scope, rendering its implementation questionable**. The consequent **designation of competent authorities is equally diverse** throughout the EU, including authorities that in some Member States may be considered as administrative and in others as criminal. Furthermore, the cooperation between national authorities and European agencies and bodies is contingent on a plethora of applicable data protection rules, which may lead to a **fragmented and asymmetrical application of data protection rules**.

Further guidance and a more harmonised approach is needed for a more straightforward delineation between the LED and the General Data Protection Regulation (GDPR) in practice, while any divergence from the core EU data protection framework, that is GDPR, LED and EU Data Protection Regulation (EUDPR), should be specifically justified, as well as strictly regulated and applied in order to avoid fragmentation.

Within Article 4, the lack of reference to the principle of transparency, the **different articulation** of the data minimisation principle, and the purpose limitation principle applied in relation to law enforcement purposes should be further contextualised in order to ensure a high level of protection of personal data. Article 4(2) has sparked academic debate due to its **lack of clarity** on how to distinguish between different law enforcement purposes and the **absence of any reference to the compatibility requirement**. The ambiguity is left to be clarified by national laws and practice which **should be closely monitored**.

Practical difficulties and national divergences from the LED wording and partial implementations have been documented as regards time limits under Article 5, as well as the categorisation of personal data under Articles 6 and 7. The legal frameworks allowing personal data, initially collected for law enforcement authorities, to be processed for non-law enforcement purposes, are reportedly currently missing.

Insofar as processing of special categories of personal data is concerned, the interrelation between Articles 10 and 8 should be further clarified and the implementation of Article 10 into national laws must be individually examined. The provision prohibiting automated decision making (Article 11) faces **several shortcomings**, affording Member States the great responsibility and discretion in addressing them.

National laws regulating processing activities by competent authorities, specifying which authority is competent to process what personal data, including the potential processing of special categories of data, for which task and purpose under Articles 8-10 must be further examined. Given the rising development and deployment of **novel technologies**, it is important to examine whether Member States have laws in place regulating their use. For instance, Member States claiming a lawful use of Pegasus for LED purposes should at least prove its compliance with the LED pursuant to Articles 4 and 8 LED. A notable number of pending cases on the interpretation of the above provisions should lead to further clarity and legal certainty.

Concerns have been raised with respect to Article 13, the information requirements therein, and the **absence of a notification duty** in line with European case law. Ambiguity has been reported regarding the right to restriction, which should be implemented by Member States as a distinct right. Although a restriction of rights should be counter-balanced through the possibility of indirect exercise of rights by the supervisory authority, **theoretical and practical difficulties** have been pointed out. Additionally, Article 17 has been erroneously transposed in a few Member States.

As Article 18 significantly limits data subject's rights allowing for national divergencies, a detailed overview of the transposition of Chapter III within Member States, including federal regimes and national criminal procedural law provisions, should be provided. The LED offers a wide discretionary power to Member States when it comes to **data subject's rights**, and reports on national transposition paint a **troubling picture**; more effort should be put both in providing information and in handling data subject's rights requests. While further guidance on the modalities for exercising data subject's rights from national and European bodies is encouraged, recent reports do show a **heightened awareness on data protection** within criminal justice.

Concerns have also been raised regarding the **opacity and lack of accessible information** regarding joint controllership in Article 21, which is compounded further by the **inconsistent national implementation** of the establishment of a single point of contact. The implementation of logging mechanisms pursuant to Article 25 stands to improve the accountability of data controllers should receive regular and continuous attention, which appears **difficult and slow-going**. Additionally, certain aspects of the logging requirement are **prone to misinterpretation** and national details on the use and management of logs appear limited despite previous recommendations. While system logs are to be used proactively, caution is due to avoid that they are processed for unrelated purposes.

Regarding the Data Protection Impact Assessment (DPIA), the comparatively limited detail provided in Article 27 remains a **serious cause for concern**, exacerbated by the various **unclarified concepts and a significant lack of concrete guidance** on DPIAs in the context of law enforcement and criminal justice. Leaving the interpretation and application of this process to the discretion of national competent authorities and supervisory bodies risks undermining its utility.

The LED contains robust requirements for data security. While it might be preferable for all Member States to have implemented the extensive list of controls provided for by Article 29 LED, high standards for data security appear to be present in national law. Nevertheless, discrepancies exist with regards to the application of these provisions at the national level and further harmonization of data breach procedures is recommended.

Questions have also been raised regarding the alignment of the prior consultation of the supervisory authority pursuant to Article 28 LED with recent EU case law on prior review of data access by law enforcement, as well as on the **apparent discrepancies** in the national interpretation and implementation of several aspects of this provision.

The **comparative lack of adequacy decisions** under Article 36 and the possible difficulties in detaching them from the GDPR's divergent scope and considerations risk **undermining a cornerstone of international transfers by competent authorities** and **weakening the protection of EU fundamental rights beyond the Union's borders**. It is recommended that the adoption of additional adequacy decisions is prioritized further. Additionally, Article 37 assigning competent authorities with the responsibility of assessing whether 'appropriate safeguards' that provide in an 'essentially equivalent' level of data protection are in place poses **serious threats to a consistent and robust framework of transfers** that provides in adequate protection for the rights of EU data subjects, thus indicating that further action may be warranted to align national standards. Diverging understandings exist regarding the place of Article 39 on the transfers to private entities in third countries in the structure of Chapter V, while its national implementation, albeit optional, appears difficult.

Concerns have been raised regarding the extent of the functional and practical independence of supervisory authorities in the context of law enforcement, given the notably lower standards than the GDPR. It is of critical importance that supervisory authorities operate in an entirely independent manner and are provided with the resources to exercise their mandate and enforce the data protection standards imposed by the LED. While national legislation implementing Articles 46 and 47 LED frequently expands upon the Directive's minimum standards, it remains regrettable that supervisory authorities are granted less extensive powers, especially in light of **CJEU case law** and **the recommendations of data protection bodies**. In addition, the exemption of courts and, optionally, independent judicial authorities acting in their judicial capacity **risks undermining robust oversight of processing operations** as few Member States appear to have introduced an effective alternative. Lastly, criticisms have been voiced regarding the **potential lack of engagement and cooperation between supervisory authority** in this sphere.

In the light of these findings the study proposes the following **recommendations**:

Member States:

- Clearer specification of scope:
    - Restrict law enforcement purposes to purely criminal justice matters, that is reconsider the application of the LED in relation to offences and authorities that may not be strictly criminal or that may be considered as administrative in most other Member States;
    - Clarify scope of application vis-à-vis courts and judicial authorities
- Data minimisation: strongly encourage 'not excessive' be interpreted narrowly, in line with the Charter, EU case law and international data protection instruments.
- Storage limitation: clear criteria for setting time frames accompanied by procedural requirements (for example oversight, Data Protection Officer).
- Include safeguards for minors and other vulnerable groups

- Data subject's rights: It is encouraged to provide information under Article 13(2) proactively and in general, not only in specific cases.
- Timeframes for reacting to data subject's rights' request should be defined in national laws and not by individual controllers.
- Establish restriction of processing as standalone right.
- Ensure effective indirect exercise of rights by the supervisory authority.
- Article 17 should not function as an alternative to direct exercise of rights nor be assimilated with the process of lodging a complaint before the supervisory authority.
- Place further emphasis on providing a greater degree of consistency, transparency and clarity with regards to the arrangements between joint controllers, in particular on the establishment of a single point of a contact and the availability of information to data subjects.
- Expand the tasks and powers conferred to the supervisory authorities under the LED by further aligning them with those under the GDPR.
- Explore alternative measures to implement oversight of compliance with data protection norms by courts and independent judicial authorities when acting in their judicial capacity.
- Broaden the extent of cooperation between independent supervisory authorities under the LED and further encourage their involvement in or contribution to the European Data Protection Board.

National competent authorities:

- Transparency: ensure significant degree of transparency, albeit adapted to specific needs of each authority, keeping in mind that not all LED subject processing activities are in need of protection from publicity but on the contrary some must be made available to the public
- Purpose limitation: Support application of purpose limitation principle with impact assessment and design tools.
- Data categorisation:
    - Categories should not be static but adaptable, otherwise it defeats the purpose of these provisions;
    - Different safeguards, including time limits, for different categories of data subjects may be encouraged, especially for vulnerable data subjects or non-suspects, insofar as practically possible;
    - Should practice reveal that this provision cannot be practically be enforced, consider alternatives following the Europol system or other (pre-existing) systems developed by European bodies or national competent authorities.
- Automated decision making and AI: competent authorities should look for national, international or European certified/auditable systems and not opt for technologies that are subject to legal constraints excluding the provision of explanations on how a system works.
- Narrow interpretation of data subject's rights restrictions:
    - The LED does not allow a blanket restriction, in other words data subject's should be informed of any processing activity relating to them as soon as the condition of restriction no longer applies, even without prior request, in line with jurisprudentially established notification duty.
    - Any derogation from the LED data subject's rights where personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings should not result in lower standards of protection
- Facilitate information to be made available and data subject's rights.
    - For example through single points of contact and/or dedicated websites including all required information as well as template for requests;
    - Abolish requirements not clearly foreseen in national laws or against spirit of LED

- Information on automated-decision making, albeit not explicitly required under Article 14, should be provided in line with Article 11 and Recital 38.

National supervisory authorities:

- Assign high priority to the processing operations by law enforcement and allocate sufficient manpower and resources to the monitoring of the LED.
- Provide more extensive guidance in the context of data protection impact assessments that is tailored to the domain of law enforcement and takes into account its unique nature while aligning the applicable standards with the greater level of detail provided by the GDPR.
- Engage in further cooperation with other supervisory authorities in the EU and sufficiently contribute to the activities of the EDPB.

EU legislator and policy bodies, including the European Commission, European Data Protection Supervisor and European Data Protection Board:

- Guidance on delineation with GDPR:
  - Further clarity on definition of 'criminal' offences, and by consequence the authorities that should be covered by the LED.
  - Harmonised approach for authorities found on the basis of EU law, such as Financial Information Units.
- Clearer alignment with Area of Freedom, Security and Justice data protection framework:
  - Reconsider application of EUDPR Chapter IX at least main principles and obligations, instead of body/database etc-specific rules or otherwise provide further guidance on alignment and application of different data protection frameworks. Any divergence from the core data protection framework, that is GDPR, LED and EUDPR, should be specifically justified, as well as strictly regulated and applied.
- Guidance on controversial provisions:
  - Purpose limitation: Further guidance on Article 4(2), what 'subsequent processing' means and how to assess compatibility of law enforcement purposes, especially in light of potentially divergent national implementations given broad discretion, ensure alignment with Charter;
  - Automated decision-making: Further elaborate upon and specify the concepts of 'automated decision-making solely based on automated means, including profiling' as well as 'human intervention', for instance taking into account the different stages involved before a decision produces effects on the individual, and by establishing a requirement of reasoned scrutiny for human intervention to be meaningful.
- Encouraged strong oversight and guidance with regards to:
  - Exercise of data subject's rights and restrictions;
  - National implementation of logging requirements regarding the adherence to the envisioned timeline for the integration of technical logging measures as well as the provision of further clarity regarding the management, supervision, use and storage of logs;
  - The conducting of DPIAs in accordance with the LED, while taking into account its unique nature as delineated from the GDPR, and encouraging further alignment of the DPIA requirements under the LED with the more extensive level of detail provided in the GDPR;
  - National observance of full independence of supervisory authorities, both through the provision of adequate resources and financial means, as well as precautions against outside interference by entities such as political institutions and law enforcement agencies;

  - National implementation of requirements for the establishment and functioning of supervisory authorities to avoid divergences from the strong safeguards provided by the LED.

- Efforts on transfers to third country recipients:
  - Examine and consider the desired extent of detail provided by national law with regards to the adherence to data security standards in law enforcement and criminal justice processing;
  - Emphasize the adoption of future adequacy decisions in accordance with the LED in order to establish a robust framework of adequacy decisions serving as a consistent and legally sound basis for third country transfers while accounting for the unique nature of law enforcement processing and decoupling this process from the motivations behind the GDPR;
  - Improve the legal certainty and provide further clarity surrounding third country transfers under appropriate safeguards in order to avoid diverging national interpretations;
  - Issue additional guidance to competent authorities with regards to key concepts such as essential equivalence;
  - Examine the envisioned responsibilities held by competent authorities in assessing data protection standards and human rights guarantees when transferring personal data to third countries;
  - Clarify various aspects relating to the exceptional transfers to non-competent recipients in third countries, including the interpretation of the role of such transfers in relation to the general structure of Chapter V.

- Continuous monitoring and assessment of implementation of LED provisions by the European Commission:
  - collection of wide range of data from a variety of sources, including the different entities that fall under the definition of competent authority under Article 3(7) LED, the national data protection supervisory authorities, civil society organisations and citizen representations, as well as EU institutions and relevant EU agencies;
  - The evaluation should be performed on the basis of the two primary objectives of the LED, that is the protection of citizens' fundamental rights and freedoms, particularly the right to the protection of personal data, and the unrestricted exchange of personal data by competent authorities within the EU.

1. INTRODUCTION AND GENERAL INFORMATION

KEY FINDINGS

The LED was adopted in order to provide for high standards of data protection and support the free flow of data in the law enforcement and criminal justice sector. However, it should not be forgotten that the LED constitutes an instrument of minimum harmonisation; it must be transposed into national laws and it often affords broad discretion to Member States, risking divergent implementations.

This study analyses the LED framework and its implementation amongst Member States, as discussed in available sources, and seeks to identify shortcomings and explore potential ways forward. A preliminary version of the study was submitted in February 2022 in order to inform the European Parliament in relation to the evaluation and review of the Directive by the European Commission by 6 May 2022.

With a regrettable delay of more than two months, the European Commission published its first report on application and functioning of the LED on 25 July 2022. It consists of a brief document prepared on the basis of a variety of sources from EU institutions, national supervisory authorities and civil society organisations.

1.1 Background and context

The protection of individuals with regards to the processing of their personal data has long been an important part of European Union (EU) law. It is enshrined as a fundamental right under Article 8 of the Charter of Fundamental Rights of the EU (Charter)[1] and in Article 16 of the Treaty on the Functioning of the European Union (TFEU)[2]. In 2016, the so-called EU data protection reform package, comprising the General Data Protection Regulation (GDPR)[3] and the Law Enforcement Directive (LED)[4] was adopted. Both these legal instruments brought numerous changes, significantly enhancing the protection of personal data within the EU. This study focuses on the LED, which repealed Council Framework Decision 2008/977/JHA (CFD)[5].

The CFD governed the processing of personal data in criminal justice cross-border situations. Its framework has been criticised for being limited in scope and binding power, and for resulting in a fragmented application of data protection rules for law enforcement authorities amongst Member States.[6] Prior to the CFD, data protection rules and principles within the field of criminal justice were

1 Charter of Fundamental Rights of the European Union ('Charter') (OJ C 202, 7.6.2016, p. 391).

2 Treaty on the Functioning of the European Union ('TFEU') (OJ C 202, 7.6.2016, p. 47).

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – 'GDPR') (OJ L 119, 4.5.2016, p. 1).

4 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 ('LED') (OJ L 119, 4.5.2016, p. 89).

5 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters ('CFD') (OJ L 350, 30.12.2008, p. 60).

6 See amongst others De Hert, P. and Papakonstantinou, V., 'The New Police and Criminal Justice Data Protection Directive: A First Analysis', *New Journal of European Criminal Law*, Vol. 7, No. 1, 2016, pp. 7–19; Marquenie, T., 'The Police and Criminal

first laid down in 1987 in the Council of Europe Recommendation R(87) 15 (Recommendation R(87) 15) [7] regulating the use of personal data in the police sector and complementing Convention 108 for the protection of individuals with regard to automatic processing of personal data[8]. Although Recommendation R(87) 15 elicited the development of national rules on data processing by law enforcement authorities, they were similarly divergent in practice.[9]

The LED seeks to remedy shortcomings from the previous CFD framework and balance the free flow of personal data between competent authorities with a consistent and high level of protection of personal data and individuals' rights and freedoms. In that vein, the new framework is adapted to accommodate the special characteristics and needs of police and criminal justice personal data processing. It has further been praised for broadening the scope of data protection rules beyond the cross-border setting and to domestic processing activities, and for providing stronger safeguards for data subjects.[10]

Nevertheless, it is worth emphasising that, although prompted by the fragmented legal landscape on data protection within criminal justice, the LED constitutes an instrument of minimum harmonisation. The choice of a directive, and the often broad discretion afforded to Member States, which may also apply higher standards of protection[11], risk the perpetuation of divergent implementations at national level.[12] Apart from legal uncertainty for controllers and data subjects, differences on data protection rules may also hinder the effective co-operation between authorities of different Member States. In addition, the LED does not apply to EU institutions, agencies, offices and bodies[13], while relevant legal acts and international agreements remain in force until amended, replaced or revoked.[14] The process

Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340.

7 Council of Europe, Committee of Ministers, Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, 17 September 1987 ('Recommendation R(87) 15').

8 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Strasbourg, 28.01.1981 ('Convention 108').

9 Cannataci, J. A. and Caruana, M. M., 'Recommendation R (87) 15 – Twenty-Five Years down the Line', Council of Europe, Strasbourg, T-PD(2013)11, 18 February 2014.

10 Colonna, L., 'The New EU Proposal To Regulate Data Protection in Law Enforcement Sector: Raises the Bar But Not High Enough', *IRI Promemoria*, Institutet för rättsinformatik, Juridiska fakulteten, Stockholms universitet, Stockholm, 2012; De Hert, P. and Papakonstantinou, V., 'The New Police and Criminal Justice Data Protection Directive: A First Analysis', *New Journal of European Criminal Law*, Vol. 7, No. 1, 2016, pp. 7–19; Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340; Leiser, M. and Custers, B., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78.

11 According to Article 1(3) of LED, '[t]his Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities'.

12 European Data Protection Supervisor, 'Opinion on the Data Protection Reform Package', 12 March 2012; Colonna, L., 'The New EU Proposal To Regulate Data Protection in Law Enforcement Sector: Raises the Bar But Not High Enough', *IRI Promemoria*, Institutet för rättsinformatik, Juridiska fakulteten, Stockholms universitet, Stockholm, 2012; Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340; Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70.

13 Article 2(3)(b) of LED.

14 Articles 60-61 of LED.

of the Commission to align third pillar acquis instruments with the LED is ongoing.[15] The question whether a desired or sufficient degree of harmonisation has been achieved is thereby raised.

Finally, the transposition of the LED into national laws has suffered several blows. In particular, the European Commission had initiated infringement procedures against 19 Member States in July 2018 for failing to adopt laws transposing the LED by the required deadline, while another procedure for partial non-transposition was initiated in July 2019.[16] The procedures were gradually closed by 2020. In 2021, the Commission referred its infringement action against Spain for failure to transpose the LED to the Court of Justice of the European Union (CJEU), which imposed both a lump sum and a penalty payment.[17] In April 2022 the Commission initiated infringement procedures against Germany, Greece, Finland and Sweden.[18] The procedure against Germany concerns a gap in the transposition of the LED in relation to the activities of Germany's federal police. The case against Greece relates to a number of points, including, the actors subject to the LED and the transposition of Articles 5, 8 and 11 LED. The cases before Finland and Sweden were initiated because the national laws do not provide data subjects with access to an effective remedy before a court or a tribunal.

1.2 Objectives, structure and methodology

As foreseen in Article 62 LED, the European Commission must evaluate and review the LED by 6 May 2022, and every four years thereafter. Particular attention should be paid to the application and functioning of Chapter V on data transfers to third countries and international organisations. In performing its task, the Commission shall take into account the positions and findings of the European Parliament, of the Council and of other relevant bodies or sources.

With a regrettable delay of more than two months, the European Commission published its first report on application and functioning of the LED on 25 July 2022.[19] It consists of a brief document prepared on the basis of a variety of sources from EU institutions, national supervisory authorities and civil society organisations.[20] The Commission highlights the LED's important contribution to the harmonised protection of personal data by competent authorities within criminal justice and throughout cross-border police and judicial cooperation and to the promotion of a culture of data protection compliance amongst competent authorities.[21] However, the European Commission's report considers that experience on the application of the LED is limited, due to its belated transposition into national laws.[22] Moreover, the European Commission, albeit being responsible for monitoring the national

[15] Communication from the Commission to the European Parliament and the Council, 'Way forward on aligning the former third pillar acquis with data protection rules', COM/2020/262 final.

[16] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 8.

[17] Judgment of 25 February 2021, European Commission v Kingdom of Spain, C-658/19, ECLI:EU:C:2021:138.

[18] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 9.

[19] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022.

[20] Ibid, p. 8

[21] Ibid, p. 5-6.

[22] Ibid, p. 8.

implementation and enforcement of the LED, found it 'difficult to compile statistics on the application of the LED'.[23]

The present study aims at informing the European Parliament's positions and findings regarding the evaluation and review of the Directive, in particular its implementation and enforcement. It reflects the research carried out in order to identify possible shortcomings in the text of the LED and incorrect transpositions within national laws. It further explores ways to address these shortcomings and mitigate their consequences. To that end, specific recommendations are formulated. The study is divided into six sections, following the order of the provisions as stipulated in the LED, and concludes with a concise presentation of recommendations.

The study is based on desktop research and the review of available studies and analyses from sources from experts and academia as well as EU institutions, including the above mentioned report by the European Commission and national data protection supervisory authorities.[24] National laws as such have not been reviewed directly but only through the available sources. . An overview of national laws, as they are discussed by said secondary sources, is provided in the Annex.[25] A preliminary version was submitted in February 2022, while the final version was submitted in October 2022.

[23] Ibid.

[24] The research relied on sources primarily in English and complementary in French, Dutch and Greek.

[25] The list of national laws as reviewed by bibliographic sources includes the following Member States: Austria, Belgium, Cyprus, Czech Republic, Germany, Greece, Italy, Ireland, Luxembourg, Netherlands, Portugal and Spain.

2. SCOPE OF THE LED

KEY FINDINGS

Both the material and the personal scope of the LED are defined by virtue of terms that further rely on national legal orders, such as criminal offence, prosecution and execution of criminal offences, public security and competent authority. Reports have shown that Member States already before the adoption of the LED but also afterwards, continue to follow divergent approaches. Such lack of harmonisation results in legal uncertainty.

More specifically, albeit autonomous, currently there is no concrete EU-wide definition of what constitutes a criminal offense. The concept of public security may be subject to both broad and narrow interpretations, while national security remains a concept currently in flux and equally vague, despite recent CJEU case law. The consequent designation of competent authorities is diverse throughout the EU, including authorities that in some Member States may be considered as administrative and in others as criminal. Moreover, the cooperation between national authorities and European agencies and bodies is contingent on a plethora of applicable data protection rules, which may lead to a fragmented and asymmetrical application of data protection rules within the AFSJ.

Further guidance and a more harmonised approach is needed for a more straightforward delineation between the LED and the GDPR in practice, while any divergence from the core EU data protection framework, that is GDPR, LED and EUDPR, should be specifically justified, as well as strictly regulated and applied in order to avoid fragmentation.

2.1 Introduction

The scope of the LED has sparked a lot of discussions already from its proposal stage, as is evident from the meetings of the Commission Expert Group on the GDPR and the LED (CEG). The LED applies to processing activities when two cumulative conditions are met: the processing pursues any of the purposes stipulated under Article 1(1), and is carried out by competent authorities as defined under Article 3(7). If either of these conditions is not met, then the GDPR applies. The scope is delimited by Article 2(3) according to which the LED does not cover processing operations that fall outside the scope of EU law, and by EU institutions, bodies, offices and agencies. These positive and negative conditions of application may prove challenging in the implementation of the LED. Relevant to these aspects are the occasionally blurred lines between the LED and the GDPR, as a the LED lacks a dedicated provision clarifying its delineation from the GDPR.[26] This section analyses issues pertaining to the LED scope and points out inconsistencies and unclarities, using examples from Member States' practice.

2.2 Law enforcement purposes and definition of criminal offence

According to Article 1, the LED applies to processing operations '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'. In this way, as aforementioned the first condition for the LED to apply is for processing

[26] By contrast, the GDPR explicitly excludes from its applicability processing operations by competent authorities for the law enforcement purposes. Article 2 of GDPR.

activities to pursue purposes that are considered as 'law enforcement purposes' due to their link to criminal offences. By contrast, non-LED purposes include for instance processing for human resources or other administrative purposes.[27]

In his Opinion on a currently pending case referred to by a Bulgarian court, Advocate General (AG) Campos Sánchez-Bordona suggested that Article 1(1) LED may be divided into three overarching types of purposes.[28] More specifically, the first concerns prevention, which also encompasses the prevention of threats to public security; the second relates to investigation in a broad sense, including detection, narrow investigation and prosecution of offences; and the third objective refers to the execution of criminal offences. By contrast, the defence of the prosecution in civil proceedings, even when it contains personal data initially collected in the context of criminal proceedings, is not amongst the purposes mentioned in Article 1(1) LED and thereby falls outside its scope.[29]

Recital 12 specifies that these purposes under Article 1 concern 'police activities without prior knowledge if an incident is a criminal offence or not … such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where 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.' **This recital has raised concerns due to the lack of clarity concerning police tasks, as well as the interchangeable use of terms such as 'law and order' with 'public security' that may be relied upon to undesirably expand the scope of the LED.**[30]

The definitions of prosecution and execution of criminal penalties, which are undertaken by a broad range of competent authorities and may differ significantly at a national level depending on criminal procedural laws, are not further clarified. Recital 20 merely notes that LED 'does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings'.[31] The scope and impact of this recital is rather unclear and could be read as extending a wider margin of discretion for Member States to derogate from data protection rules.[32] **It remains unclear whether some or all phases of a criminal trial fall within the scope of the LED, while**

---

27 European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 10.

28 Opinion of Advocate General Campos Sánchez-Bordona of 19 May 2022, *Inspektor v Inspektorata kam Visshia sadeben savet*, ECLI:EU:C:2022:406, C-180/21, paragraph 52.

29 Ibid, paragraph 88.

30 Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology,* Vol. 33, No 3, 2019, pp. 249–70.

31 A similar discretion is foreseen in the GDPR, under Recital 20 which allows national regulation of processing by courts and other judicial authorities, as well as their exclusion from supervision by national supervisory authorities, as is also the case with the LED, see below under section 7.

32 Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology,* Vol. 33, No 3, 2019, pp. 249–70.

Member States are given a broad discretion in regulating data processing for courts and judicial authorities, as discussed also below under sections 4 and 7.[33]

As established in Recital 13, a criminal offence 'should be an autonomous concept of Union law' as interpreted by the CJEU. Accordingly, assessing whether an offence is criminal in nature depends on three factors: whether the offence is classified as such under national law, the intrinsic nature of the offence, and the degree of severity of the penalty that the person concerned is liable to incur.[34] Nevertheless, the interpretation by the CJEU essentially includes all definitions of what constitutes a criminal offence under the different Member State laws. The lack of more concrete harmonisation may result in offences being considered as criminal within some national legal orders and as administrative in others.[35]

During the CEG meetings, the legal service of the European Commission contended that Member States may rely on their national definition, despite the lack of consensus on the notion of criminal offence throughout the EU.[36] As evidenced during said CEG meetings, both the definition of criminal, in contrast to administrative, offences, and the criminal or administrative nature of certain authorities, such as Financial Intelligence Units (FIUs) differ across Member States (see also below under 2.4).[37] Several Member States underlined that their national systems include minor offences within their criminal law or intend to apply the LED to such offences as they may lead to criminal proceedings. Additionally, some Member States expressed their intention to apply the LED to authorities which otherwise carry out administrative tasks, where such authorities handle minor offences that may lead to criminal proceedings.[38] Distinguishing between administrative and criminal proceedings continued to be reported as a problem in more recent meetings by the CEG.[39] Moreover, Member States reportedly included purposes beyond those listed in Article 1 LED, such as the safeguarding against threats to public order or public safety.[40] Unless the CJEU provides a harmonised interpretation of criminal offence that does not rely on national law, it is likely that Member States will continue to employ their diverging national definitions.

As a matter of illustration, reference can be made to a 2020 report demonstrating that the various interpretations of police objectives and tasks amongst Member States can affect the types of authorities that may be considered part of law enforcement, including border police, transport police,

---

33 See also Brewczyńska, M., '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 Kosta and Leenes (eds) *Research Handbook on EU data protection* (Edward Elgar 2022).

34 Judgment of 22 June 2021, *B v Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504, paragraph 87.

35 Commission Expert Group, Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4 May 2017, paragraph 1

36 Commission Expert Group, Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4 May 2017, paragraph 1.

37 Commission Expert Group, Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 November 2016; Minutes of the fifth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 18 January 2017; Minutes of the seventh meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 March 2017 and Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4 May 2017.

38 Ibid.

39 Commission Expert Group, Minutes of the meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 5 May 2021.

40 European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 11.

public safety, and administrative police[41] (see also below under 2.3). For instance, the German implementation of the LED has also been rendered applicable to the so-called *Ordnungswidrigkeiten,* which constitute non-criminal offenses that are subject only to administrative sanctions in the form of a monetary fine. As noted in the report, this is a legal concept that is not similarly present or understood as such in most of the EU Member States. Its inclusion under the scope of the German law could thus deviate from the legal practice observed in countries that employ a more narrow interpretation of a criminal offense and that might not consider similar administrative sanctions to fall under their implementation of the LED.

By consequence, the ambiguous delineation of law enforcement purposes and the different national definitions of criminal offence may impact on the scope of the LED and result in diverging application amongst Member States.

2.3 Competent authorities

The uncertainty veiling the material scope of the LED further impacts on the determination of its personal scope as hinted above. Pursuant to Article 3(7)(a) LED, a competent authority may be any public authority 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. As aforementioned, different understandings of 'criminal offence' and 'public security' may lead to different types of national authorities falling within or outside the scope of the LED. Moreover, under Article 3(7)(b) LED, a competent authority may be any other body or entity entrusted by Member State law to exercise public authority and public powers for the same law enforcement purposes. According to the CJEU, a competent authority 'must be understood in relation to the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, in view of the arrangements which may prove necessary, in that regard, because of the specific nature of those fields'.[42]

During the proposal phase, both European Data Protection Supervisor (EDPS) and Article 29 Working Party (WP29) raised their concerns about a potential expansion of applicability of the LED upon authorities which would otherwise fall under the GDPR framework, as this second type of competent authority under Article 3(7)(b) may also include administrative or private entities not strictly related to criminal justice matters.[43] The determination of this second type of competent authorities is largely contingent on the definitions of public security, public authority and public power, which rely on each Member State's national legal order. In its 2022 report, the European Commission referred to competent authorities under Article 3(7)(b) LED as 'private bodies, on which the law confers special powers beyond those which result from the normal rules applicable in relations between individuals and/or by the possibility of exercising the power of coercion'.[44] Interestingly, in its ruling on the

[41] Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020, p. 33.

[42] Judgment of 22 June 2021, *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504, paragraph 70.

[43] European Data Protection Supervisor, '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', 28 October 2015 ; Article 29 Data Protection 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 or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015.

[44] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 10.

Passenger Name Record (PNR) Directive[45], the CJEU excluded private entities, such as air carries, from the scope of the LED because they are 'neither in charge of exercising public authority nor entrusted with public powers by that directive'.[46] Such understanding implies that in a field regulated by EU law, it is the EU law that should appoint such public power or authority upon a private body to fall under the Article 3(7)(b) definition of competent authority, rather than the Member State transposing the legal instrument in question.

As documented, Member States have followed divergent approaches, some listing the competent authorities explicitly within their national laws, while others opting for either more limited or broader definitions.[47] More specifically, Bulgaria[48] and Greece[49] adopted a restrictive terminology by referring to state bodies, thereby excluding any private entity from the scope of the LED. In that regard, the Greek supervisory authority opined that this approach goes against the wording of the LED.[50] The German Federal Act includes several public and private entities entrusted with public security under the scope of the GDPR.[51] Accordingly, the processing of personal data by public bodies is permitted for reasons of, amongst other, public interest and security, to prevent substantial harm and defence. The LED is further applicable to public bodies responsible for executing penalties, criminal measures, and educational or disciplinary measures as referred to in the Juvenile Court Act.

By contrast, several Member States decided to designate a broad range of public and other authorities as competent within the meaning of the LED. For instance, the Irish supervisory authority considers local authorities when prosecuting litter fines or public transport companies processing ticket offences as potentially falling under the definition of competent authorities within the Irish law transposing the LED.[52] French competent authorities may include the safety internal services of critical infrastructure authorities such as the Autonomous Operator of Parisian Transports (Régie Autonome des Transports Parisiens – RATP) and the French National Railway Company (Société nationale des chemins de fer français – SNCF), and the approved sports federations for the purpose of securing sports events consist of competent authorities.[53]

---

45 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime ('PNR Directive') (OJ L 119, 4.5.2016, p. 132).

46 Judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, ECLI:EU:C:2022:491, paragraph 81.

47 Vogiatzoglou, P. and Fantin, S., 'National and Public Security within and beyond the Police Directive', Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructures, ed. Anton Vedder et al., 1st ed., KU Leuven Centre for IT & IP Law Series 7, Intersentia, Cambridge, Antwerp, Chicago, 2019, pp. 27–62.

48 Panteleeva, V., 'Transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 in Personal Data Protection Act in Republic Of Bulgaria', *Legal Science: Functions, Significance and Future in Legal Systems II*, The 7th International Scientific Conference of the Faculty of Law of the University of Latvia, 16–18 October 2019, Riga, Collection of Research Papers, pp. 210-217.

49 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Greek supervisory authority), Γνωμοδότηση 1/2020, Athens 24 January 2020.

50 Ibid.

51 Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).

52 An Coimisinéir Cosanta Sonraí – Data Protection Commission (Irish supervisory authority), 'Law Enforcement Directive, Guidance on Competent Authorities and Scope', available at https://www.dataprotection.ie/en/organisations/resources-organisations/law-enforcement-directive.

53 Commission nationale de l'informatique et des libertés (French supervisory authority), '"Law Enforcement Directive": What Are We Talking About?', 2 June 2021, available at: https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about.

The Belgian list of competent authorities includes the General Administration of Customs and Excise, the Passenger Information Unit, the Financial Information Processing Unit and the Investigation Service of the Standing Committee for the Control of Intelligence Services in the framework of it judicial missions.[54] Similarly, the Spanish list of competent authorities includes the Deputy Directorate of the Customs Surveillance Service, the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offenses, and the Commission for the Surveillance of Terrorism Financing Activities.[55] Finally, the Italian legislator made explicit that competent authorities may be Italian, European or third-country ones, while the Italian transposition of Article 3(7)(b) refers to any other entity or organization tasked by the national legal system with law enforcement activities, allowing for a broad interpretation of competent authorities.[56] The expansive approach followed by these Member States demonstrates how any national law can designate entities as competent authorities within the meaning of the LED, without a requirement of public authority and power, thereby widening the LED scope of application.[57]

There are many reasons why a disjointed understanding of what constitutes a competent authority throughout the EU may be problematic.[58] First, the LED, due to its dual aim to safeguard both fundamental rights and the free flow of personal data within the context of criminal justice, allows a wider margin of discretion and in certain areas is more lenient than the GDPR. Any broadening of its scope should thereby be limited in the spirit of the LED and its objectives. As noted by the EDPS and WP29 during the proposal phase, the notion of competent authorities should be interpreted as limited as possible in order to ensure a high level of protection of personal data.[59] Second, it creates legal uncertainty and fragmentation with respect to the applicable data protection rules across the EU, which may further impede data subjects who wish to exercise their rights.

2.4 Public and national security

Another challenging element of the LED scope concerns the inclusion of 'the safeguarding against and the prevention of threats to public security' within the scope of the LED, which was added by the Council during the proposal phase and was met with severe criticism. In particular, both EDPS and WP29 drew attention to the lack of clarity surrounding the concept of public security, often broadly

---

54 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018).

55 Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (Boletín Oficial del Estado 126/2021-05-27, p. 64103). See also Quezada Tavárez, K., 'Highlights of the Spanish Act on Data Protection in the Area of Police and Criminal Justice (Organic Law 7/2021)', CiTiP Blog,15 June 2021, available at https://www.law.kuleuven.be/citip/blog/highlights-of-the-spanish-act-on-data-protection-in-the-area-of-police-and-criminal-justice/.

56 Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15 (Gazzetta Ufficiale della Repubblica Italiana 61, 14 March 2018).

57 Fantin, S., 'Law enforcement and personal data processing in Italy: implementation of the Police Directive and the new data retention law', CiTiP Blog, 29 May 2018, available at https://www.law.kuleuven.be/citip/blog/law-enforcement-and-personal-data-processing-in-italy-implementation-of-the-police-directive-and-the-new-data-retention-law/.

58 See also Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340.

59 European Data Protection Supervisor, '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', 28 October 2015 ; Article 29 Data Protection 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 or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015.

interpreted, resulting in a risk of expansion of the LED scope beyond purely criminal justice matters.[60] To complicate matters even more, the LED applies to processing activities in pursuit of public security but not in pursuit of national security.[61]

National and public security comprise vague and broad concepts that may be interpreted differently on a national, European and international level.[62] On the one hand, the notion of national security is traditionally linked to state sovereignty, relates to essential State functions and fundamental interests of society[63], and may assume several general characteristics. A few Member States provide for explicit definitions of national security within their national legal orders, including Bulgaria, Spain, Hungary, Italy and Luxembourg.[64] For instance, the Hungarian definition of national security includes disruption of democracy, terrorism and trafficking, the Italian definition includes the safeguarding of internal security, from 'any threat, any subversive activity and any form of criminal or terrorist aggression' and the Luxembourgish definition includes the security of institutions, fundamental rights, and economic interests.[65] In fact, some Member States, like Cyprus, Czech Republic, Hungary, Italy, Luxembourg, Malta, Spain and Romania, understand national security as intertwined with public security, including aspects such as the fight against organised crime and terrorism, as well as the safeguarding of financial interests and internal security.[66] The CJEU itself refers to the protection of national security as encompassing the 'prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities'.[67]

In the EU legal order, while national security remains the sole responsibility of the Member States[68], it must be interpreted strictly[69] and it does not automatically render any related activity outside the scope of EU law, as confirmed recently by the CJEU Privacy International and La Quadrature du Net rulings. More specifically, according to the CJEU, the national security exception is applicable only when it concerns practices that are purely governmental, that is without the involvement of any private actor.[70] If national measures impose obligations upon individuals such as electronic communications services

---

60 European Data Protection Supervisor, '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', 28 October 2015, p. 5; Article 29 Data Protection 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 or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015, p. 5.

61 Article 2(3)(a) of LED and Recital 14 of LED.

62 Vogiatzoglou, P. and Fantin, S., 'National and Public Security within and beyond the Police Directive', *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructures*, Vedder, A. et al. (eds), 1st ed., KU Leuven Centre for IT & IP Law Series 7, Intersentia, Cambridge, Antwerp, Chicago, 2019, pp. 27–62; Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70.

63 Judgment of 22 June 2021, *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504, paragraph 67.

64 Rijpma, J. et al. (eds), The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection, the XXIX FIDE Congress in The Hague 2020 Congress Publications, vol. 2, Eleven International Publishing, the Hague, 2020.

65 Ibid.

66 Ibid.

67 Judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 135.

68 Article 4(2) of Treaty on European Union (OJ C 202, 7.6.2016, p. 15).

69 Judgment of 22 June 2021, *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504, paragraph 62.

70 Judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 35; Judgment of 6 October 2020, *La Quadrature du Net and Others,* C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 92.

providers (ECSPs), in pursuit of national security in line with Article 15(1) E-Privacy Directive (EPD)[71], then they fall within the scope of EU law.[72] Although the rulings in question concerned the applicability of the EPD and the GDPR, this delineation of national security activities not falling outside the scope of EU law will most likely also have an impact on the implementation of the LED amongst Member States. This judicial line of reasoning may open the doors for the LED to apply on certain processing operations even in pursuit of national security interests.[73]

On the other hand, public security has undertaken a dynamic role within EU law. In several fields of EU law, including the Area of Freedom, Security and Justice (AFSJ)[74] and data protection, public security has long functioned as an exception allowing divergence from the applicability of EU law. The CJEU has followed an expansive interpretation of public security, as encompassing elements traditionally considered to be part of national security, such as the safeguarding of the functioning of institutions, military interests and the fundamental interests of society.[75] The latter has also been included in Recital 12 of the LED. According to the CJEU, a threat to national security is 'distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed'.[76] However, as the Court often uses similar terms to describe the nature of threats to national and public security, the most decisive factor seems to be a temporal one; threats to national security must be 'present or foreseeable' while threats to public security are characterised as 'general'. Still, the lines between foreseeable and general may too get easily blurred. **The ambiguity surrounding the clear delineation between the concepts of public and national security may also result in diverging implementation of the LED.**

Of course, as Member States are allowed to provide for higher standards of protection beyond the LED, they may extend its applicability to processing activities also in pursuit of national security.[77] In fact, some Member States apply data protection rules to processing operations by authorities such as intelligence services for the safeguarding of national security, including Belgium, Czech Republic, Finland, France, Hungary, Luxembourg, Netherlands and Slovenia.[78] By contrast, Poland, excludes the

---

71 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 (Directive on privacy and electronic communications – 'EPD') (OJ L 201, 31.7.2002, p. 37).

72 Judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraphs 39, 41; Judgment of 6 October 2020, *La Quadrature du Net and Others,* C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 96, 98.

73 Kosta, E., 'A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon', *Research Handbook on EU data protection*, Kosta, E. and Leenes, R. (eds), Edward Elgar, 2022 (forthcoming).

74 Title V of TFEU.

75 Judgment of 23 November 2010, *Land Baden-Württemberg v Panagiotis Tsakouridis*, C-145/09, EU:C:2010:708, paragraph 44; Judgment of 22 May 2012, *P.I. v Oberbürgermeisterin der Stadt Remscheid*, C-348/09, EU:C:2012:300, paragraph 28.

76 Judgment of 5 April 2022, G*.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, ECLI:EU:C:2022:258, paragraph 62.

77 See also Commission Expert Group, Minutes of the fifteenth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 20 February 2018.

78 On Czech Republic, Finland, Luxembourg, Netherlands and Slovenia see Rijpma, J. et al. (eds), *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, the XXIX FIDE Congress in The Hague 2020 Congress Publications, vol. 2, Eleven International Publishing, the Hague, 2020. On Belgium see Vogiatzoglou, P., Quezada Tavárez, K., Fantin, S. and Dewitte, P., 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives', *Journal of Intellectual Property, Information Technology and E-Commerce Law,* Vol. 11, No 3, 2020, pp. 274–302. On France see Commission nationale de l'informatique et des libertés (French supervisory authority), '"Law Enforcement Directive": What Are We Talking About?', 2 June 2021, available at: https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about. On Hungary see Chambers and Partners, *Data Protection & Privacy 2021, Practice*

applicability of EU data protection rules for a broad range of activities, even those that have nothing to do with national security or those that would fall under public security and thereby should be subject to the LED transposition.[79] In particular, the Polish transposition of the LED does not apply to personal data processed in connection with the provision of national security, including the statutory tasks of the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence and the Central Anti-Corruption Bureau.[80] As reported by Rijpma et al, '[a]ccording to the doctrine, these exclusions are not only too broad in the absence of a definition of the term "national security", but also include institutions whose activities go far beyond the common understanding of the term'.[81] Finally, Portugal has reportedly adopted a provision to restrict LED data subject rights on the basis of national security, which might create a confusion as to the scope of the national law transposing the LED.[82]

2.5 Between the LED, the GDPR and AFSJ-specific frameworks

As mentioned, the LED applies only when both material and personal conditions of application are fulfilled. In other words, it does not apply when competent authorities process personal data for non-law enforcement purposes, nor when entities other than competent authorities process personal data for law enforcement purposes. The LED is considered as the more specific legal act in relation to the GDPR which defines the general rules.[83] Any processing operation outside the scope of the LED (and still within the scope of EU law) is subject to the GDPR, Regulation (EU) 2018/1725 (EUDPR)[84] or other sector specific instrument.

Between LED and GDPR

As hinted throughout the previous analyses, however, the lack of clarity surrounding the core notions of the LED scope complicates its delineation from the GDPR. During the first CEG meeting, Member States raised their concerns on how to definitively delineate between the LED and the GDPR, an issue that remained to an extent unresolved throughout these meetings.[85] Particularly challenging are situations where the designation of authorities as competent is not straightforward or where processing activities are transitioning from the GDPR to the LED framework, for instance during data transfers from companies to public authorities for law enforcement purposes.

Guides, Hungary, last updated 09 March 2021, available at: https://practiceguides.chambers.com/practice-guides/comparison/627/6267/10386-10395-10401-10406-10414

79 Rijpma, J. et al. (eds), *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, the XXIX FIDE Congress in The Hague 2020 Congress Publications, vol. 2, Eleven International Publishing, the Hague, 2020.

80 Article 3(2) of U S T AWA z dnia 14 grudnia 2018 r.o ochronie danych osobowych przetwarzanych w zwi±zku z zapobieganiem i zwalczaniem przestępczo.

81 Rijpma, J. et al. (eds), *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, the XXIX FIDE Congress in The Hague 2020 Congress Publications, vol. 2, Eleven International Publishing, the Hague, 2020.

82 Ibid.

83 Judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, ECLI:EU:C:2022:491, paragraph 72.

84 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 ('EUDPR') (OJ L 295, 21.11.2018, p. 39).

85 Commission Expert Group, Minutes of the first meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 23 September 2016.

The most concrete example relates to the Anti-Money Laundering (AML) Directive, and the processing of personal data by financial institutions and by national FIUs.[86] FIUs are authorities tasked by virtue of EU law to receive and process personal data from the private, financial, sector, in order to investigate suspicious transactions and contribute in the fight against money laundering and terrorist financing. As already pointed out during the CEG meetings, some FIUs are set up as administrative authorities while others as law enforcement authorities within the meaning of competent authority under Article 3(7) LED, or as hybrid entities.[87] In addition, while processing activities under the AML Directive at large are subject to the GDPR and the EUDPR[88], this does not necessarily apply to FIUs.[89] Till this day, it remains unclear whether FIUs constitute competent authorities, due to their diverging legal nature as well as in light of their evolving mandate under the EU AML framework.[90] For instance, as demonstrated above, some Member States like Belgium and Spain include FIUs amongst the LED competent authorities, as said FIUs are public authorities tasked under national law with processing activities linked to AML criminal offences and thereby fall under the definition of Article 3(7)(a) LED. In this way, the Belgian and Spanish FIUs are subject to the LED insofar as they process personal data for law enforcement purposes, and to the GDPR when their processing activities relate to non-LED purposes. By contrast, other national FIUs are only subject to the GDPR, insofar as they are not considered as competent authorities under national law.

Recital 11 LED, dedicated to shedding light to the relation between the LED and the GDPR seems to fall short, as it rather confusingly states:

> '[…] Regulation (EU) 2016/679 therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of Regulation (EU) 2016/679 remains unaffected for the processing of personal data by the processor outside the scope of this Directive.'

---

86 Article 32 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73), as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ L 156, 19.6.2018, p. 43) ('4th AML Directive as amended by 5th AML Directive').

87 Commission Expert Group, Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 November 2016. See also EUROPOL, 'From Suspicion to Action - Converting Financial Intelligence into Greater Operational Impact', Publications Office of the European Union, Luxembourg, 2017, p. 28.

88 Article 41 of 4th AML Directive as amended by 5th AML Directive.

89 Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70.

90 Brewczyńska, M., 'Financial Intelligence Units: Reflections on the Applicable Data Protection Legal Framework', *Computer Law & Security Review,* Vol. 43, 2021, pp. 105612.

On the basis of this passage, several scholars have attempted to clarify the application of the definitions of the competent authorities and of processors, as well as the boundaries between the LED and the GDPR.[91] Particularly in relation to the AML framework, it has been debated whether FIUs can act as processors within the meaning of the LED[92], as well as whether private entities such as financial institutions, mentioned in the recital, should be considered as processors under the LED, or as joint controllers under an ambiguous data protection framework, given their discretionary decisional power[93].

This debate is especially relevant for other types of public authorities and private entities involved in similar ways in the fight against crime, with most prominent examples the sectors of tax administration, air traveling and electronic communications services. Therein, a diversity of approaches are followed vis-à-vis the applicability of the LED or the GPDR. Prior to the entry into force of the reformed EU data protection package, the CJEU had found that data not collected directly for the purpose of public security or in pursuit of criminal proceedings but also used for collecting tax and combating tax fraud by state authorities, to fall under the scope of Directive 95/46[94].[95] Passenger Information Units (PIUs), which are public authorities similar to FIUs, established to receive personal data from private entities such as airlines, for law enforcement purposes, are considered as competent authorities and must abide by the LED when processing personal data for public security purposes.[96]

In the context of transfers of personal data from entities subject to the GDPR to entities subject to the LED, it has been questioned to what extent the exact processing operation of data transferring itself is subject to the GDPR or the LED.[97] Recent CJEU case law has confirmed that the act of transferring of personal data by private entities to competent authorities falls under the GDPR (and where relevant the EPD) and not the LED. More specifically, in the aforementioned Privacy International and La Quadrature du Net rulings, the CJEU made a remark concerning the delineation of scope between the LED and the GDPR. In particular, according to the CJEU, although the GDPR does not apply to processing operations by 'competent authorities' for law enforcement purposes,[98] 'it is apparent from

---

91 See for example Purtova, N., 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' *International Data Privacy Law*, Vol 8, No 52, 2018, pp. 52-68; Vogiatzoglou, P. and Fantin, S., 'National and Public Security within and beyond the Police Directive', *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructures*, ed. Anton Vedder et al., 1st ed., KU Leuven Centre for IT & IP Law Series 7, Intersentia, Cambridge, Antwerp, Chicago, 2019, pp. 27–62; Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70; Brewczyńska, M., 'Financial Intelligence Units: Reflections on the Applicable Data Protection Legal Framework', *Computer Law & Security Review,* Vol. 43, 2021, pp. 105612.

92 Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70; Brewczyńska, M., 'Financial Intelligence Units: Reflections on the Applicable Data Protection Legal Framework', *Computer Law & Security Review,* Vol. 43, 2021, pp. 105612.

93 Purtova, N., 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' *International Data Privacy Law*, Vol 8, No 52, 2018, pp. 52-68.

94 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 ('DPD') (OJ L 281, 23.11.1995, p. 31).

95 Judgment of 27 September 2017, *Puškár*, C-73/16, EU:C:2017:725, paragraphs 39-40, 44.

96 Article 13 of PNR Directive; Judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, ECLI:EU:C:2022:491, paragraphs 79-80.

97 Purtova, N., 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' *International Data Privacy Law*, Vol 8, No 52, 2018, pp. 52-68.

98 Art 2(2)(d) of GDPR.

Article 23(1)(d) and (h) [GDPR][99] that the processing of personal data carried out by individuals for those same [law enforcement] purposes falls within the scope of [the GDPR]'.[100] By contrast, the CJEU concluded, 'where the Member States directly implement measures that derogate from the [EPD], without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by [the EPD], but by national law only, subject to the application of [the LED].[101] This implies that any national or potential European legislative instrument imposing an obligation upon ECSPs to retain and transfer personal data for law enforcement purposes in line with Article 15 EDP should be subject to the GDPR and not the LED. Similarly, as aforementioned, the transferring of personal data to PIUs by airlines and other private entities under the PNR Directive are subject to the GDPR.[102]

Finally, the CJEU has clarified that, whereas Directive 95/46 did not draw any distinction as to the actor performing the processing activity in its provision on its scope, the GDPR clearly does draw such distinction.[103] The non-applicability of the GDPR, and thereby the applicability of the LED, depends, amongst other, on whether processing takes place by a competent authority under the LED meaning.[104] In this way, previous case law on the scope of Directive 95/46 may no longer be applicable on the delineation of scopes between GDPR and LED.[105]

In the era of the elaborate EU data protection framework, and taking into account the complexities analysed throughout this section, it becomes obvious that further guidance and a more harmonised approach is needed for a more straightforward delineation between the LED and the GDPR in practice and in relation to all the authorities in charge of tasks bordering between administrative and criminal flowing from national and EU law. To an extent, the CJEU has started to fill in the gaps, and potentially future case law will further clarify the interrelation between the two instruments.

Between LED and sectoral frameworks

As per Article 2(3)(b), the LED does not apply to processing operations by the Union institutions, bodies, offices and agencies. Instead, the EUDPR sets up a general data protection framework for processing activities by EU entities at large. It also provides a specific set of rules for processing of operational data[106] by EU entities when carrying out activities falling within the scope of the AFSJ. The EUDPR frameworks should be consistent with the LED.[107] In addition to this dedicated Chapter IX of the EUDPR, the processing of operational data by Europol and the European Public Prosecutor's Office (EPPO) is

[99] The provision in question outlines the permissible restrictions to the application of the GDPR in the context of amongst other national security, defence and public security.

[100] Judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 47; Judgment of 6 October 2020, *La Quadrature du Net and Others,* C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 102.

[101] Judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 48; Judgment of 6 October 2020, *La Quadrature du Net and Others,* C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 103.

[102] Judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, ECLI:EU:C:2022:491, paragraph 81.

[103] Ibid, paragraphs 66-67.

[104] Article 2(2) of GDPR.

[105] Judgment of 21 June 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491, paragraphs 65-69.

[106] Operational personal data means all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies. Article 3(2) of EUDPR, referring to Title V of Part Three of TFEU.

[107] Article 2(2) of EUDPR.

also regulated by their establishing Regulations, which must be revised accordingly.[108] At the moment, only the Regulation of Europol has been amended, stating that the Europol data processing activities are subject to the EUDPR without prejudice to the provisions specified in the new Regulation.[109] As also noted in the introduction, EU relevant legal acts already in force before May 2016 remain unaffected[110] and await revision on the basis of the ongoing Commission process.[111]

As a result, data processing by EU entities within the scope of the AFSJ will be subject to a complex framework whereby the EUDPR Chapter IX on operational data should be complemented by the agency-specific data protection rules and at the same time be consistent with the LED.[112] The fragmentation as well as the choice to subject EU entities to different data protection frameworks have been questioned, as EU institutions, bodies, agencies and offices should be bound by the same rules that apply at Member State level.[113]

Particularly insofar as Europol is concerned, not only will a separate data protection framework apply, but also the new Regulation has been criticised for legalising previously deemed illegal practices.[114] More specifically, the EDPS, upon issuing an admonishment against Europol for its processing of large datasets and lack of data protection safeguards[115], used its corrective powers by ordering Europol to delete data concerning individuals with no established link to a criminal activity.[116] Accordingly, the EDPS ordered Europol to categorise both newly received personal data within 6 months of receipt, as well as existing data within 12 months. Before being categorised, data should not be processed while after the respective periods have passed, non-categorised data should be deleted. Instead, the new Europol Regulation extended the period under which data do not need to be categorised to 18 months, which may be further extendable, and allowed non-categorised data to be in the meantime subject to processing.[117] In this way, Europol may now process personal data of individuals not categorised as having any link to crime, even at large scale. Evading the applicability of the EUDPR and providing for

[108] Article 2(3) of EUDPR.

[109] Recital 45 and Article 27a of Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation (OJ L 169, 27.6.2022, p. 1).

[110] Article 60 of LED.

[111] Communication from the Commission to the European Parliament and the Council, 'Way forward on aligning the former third pillar acquis with data protection rules', COM/2020/262 final.

[112] See also González Fuster, G., 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights', European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 656.295, 2020.

[113] Alonso Blas, D., 'Ensuring Effective Data Protection in the Field of Police and Judicial Activities: Some Considerations to Achieve Security, Justice and Freedom', *ERA Forum,* Vol. 11, no. 2, 2010, pp. 233–50; Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70.

[114] European Data Protection Supervisor, Press Statement Amended Europol Regulation weakens data protection supervision, EDPS/2022/16, 27 June 2022.

[115] European Data Protection Supervisor, EDPS Decision on the own initiative inquiry on Europol's big data challenge, 18 September 2020.

[116] European Data Protection Supervisor, EDPS Decision on the retention by Europol of datasets lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699), 21 December 2021.

[117] Article 18 of Regulation (EU) 2016/794 as amended by Regulation (EU) 2022/991.

specific data protection rules, not only fragments the landscape but also risks that insufficient safeguards are in place, as the EDPS noted with regards to the new Europol Regulation.[118]

Furthermore, one part of the AFSJ seems to be found in-between the LED, the GDPR, and sector-specific data protection frameworks. More specifically, processing operations in the area of border control, asylum and immigration are subject to the GDPR insofar as they don't relate to law enforcement purposes, to the LED from the moment they are linked to potential criminal proceedings, and to specific rules applicable for cross-border information exchanges between the competent police and judicial authorities.[119]

Lastly, if adopted, processing operations involving personal data and falling within the scope of the proposed Artificial Intelligence (AI) Act will also need to abide by all relevant frameworks, including the LED and the GDPR.[120] This will be the case for instance in the deployment of technologies such as facial recognition, algorithmically aided criminal profiling and predictive analytics[121], whereby alignment between these instruments will be crucial.[122] In that regard, there have been calls for an outright ban on more law enforcement uses of AI systems, such as certain uses of biometric identification and predictive policing.[123] The recitals of the proposed AI Act mention that the proposal is without prejudice and complements the GDPR and the LED. However, a more explicit guarantee within the body of provisions on the applicability of and necessary compliance with existing EU data protection frameworks has been requested, in order to ensure that the proposed AI Act does not lower the level of protection already provided.[124] The proposal is now undergoing discussions and amendments by

[118] European Data Protection Supervisor, Press Statement Amended Europol Regulation weakens data protection supervision, EDPS/2022/16, 27 June 2022.

[119] European Union Agency for Fundamental Rights (FRA), *Handbook on European Data Protection Law*, 2018 edition, Publications Office of the European Union, Luxembourg, 2018, p. 291-324; Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873; González Fuster, G., 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights', European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 656.295, 2020. See also for instance Chapter VII of Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

[120] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts, COM/2021/206 final (Proposed AI Act).

[121] Articles 1(d), (2)-(4), Chapters 1-2 and Annex III point 6 of Proposed AI Act.

[122] See for example Wenderhorst, C.and Duller, Y. 'Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces', PE 696.968, 2021.

[123] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021; European Parliament, Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, 2021/0106(COD), 20 April 2022.

[124] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021; Ebers M. et al., 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)', J Vol. 4, No. 4, 2021, pp. 589–603.

the co-legislators, the European Parliament and the Council, which could lead to substantial changes in the foreseen framework.[125]

Data processing operations within the AFSJ therefore face a potentially fragmented and confusing landscape of applicable data protection rules. This may further impact the exercise of data subject's right when processing operations spread across different jurisdictions, entities or databases.[126] Legal consistency and coherence in the cooperation between national competent authorities and EU institutions, bodies, offices and agencies in this area may thereby be challenging to achieve.[127] Legal and policy solutions should be further examined on an EU level.[128] Any divergence from the core data protection framework, that is GDPR, LED and EUDPR, should be specifically justified, as well as strictly regulated and applied. For instance, while the new Europol Regulation seems to allow for great discretion and deviation from the data categorisation and storage limitation rules, its compatibility with core data protection principles and its application should be strictly monitored, as also proclaimed by the EDPS.[129] Moreover, the EU legislator could in the future strive for clearer and closer alignment of sector or body specific data protection rules with the harmonising frameworks of the GDPR, LED and EUDPR, ensuring that exceptions only apply to a limited extent.

[125] For information on the legislative process, see European Parliament Legislative Train Schedule at: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence.

[126] Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' *Privacy Technologies and Policy*, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30.

[127] Colonna, L., 'The New EU Proposal To Regulate Data Protection in Law Enforcement Sector: Raises the Bar But Not High Enough', *IRI Promemoria*, Institutet för rättsinformatik, Juridiska fakulteten, Stockholms universitet, Stockholm, 2012; Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70; Kosta, E., 'A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon', *Research Handbook on EU data protection*, Kosta, E. and Leenes, R. (eds), Edward Elgar, 2022 (forthcoming); Vogiatzoglou, P., 'Article 2: Scope', *The Law Enforcement Directive: A Commentary*, Kosta, E. and Boehm, F. (eds), Oxford University Press 2022 (forthcoming – under review).

[128] See Chairman of Committee on Civil Liberties, Justice and Home Affairs, 'LIBE Contribution to the Commission upcoming report on the evaluation and review of the Law Enforcement Directive', IPOL-COM-LIBE D (2022)3535, 7 February 2022.

[129] European Data Protection Supervisor, Press Statement 'Amended Europol Regulation weakens data protection supervision', EDPS/2022/16, 27 June 2022.

3. PRINCIPLES

KEY FINDINGS

Within Article 4, the lack of reference to the principle of transparency and the different articulation of the data minimisation principle and the purpose limitation principle applied in relation to law enforcement purposes, should be further contextualised in order to ensure a high level of protection of personal data. Article 4(2) has sparked academic debate due to its lack of clarity on how to distinguish between different law enforcement purposes and the absence of any reference to the compatibility requirement. The ambiguity is left to be clarified by national laws and practice which should be closely monitored.

Practical difficulties, national divergences from the LED wording and partial implementations have been documented as regards time limits under Article 5 as well as the categorisation of personal data under Articles 6 and 7. The legal frameworks allowing personal data, initially collected for law enforcement authorities, to be processed for non-law enforcement purposes, are reportedly currently missing.

Insofar as processing of special categories of personal data is concerned, the interrelation between Articles 10 and 8 should be further clarified and the implementation of Article 10 into national laws must be individually examined. The provision prohibiting automated decision making faces several shortcomings, affording Member States the great responsibility and discretion in addressing them.

National laws regulating processing activities by competent authorities, specifying which authority is competent to process what personal data, including the potential processing of special categories of data, for which task and purpose under Articles 8-10 must be further examined. Given the rising development and deployment of novel technologies, it is important to examine whether Member States have laws in place regulating their use. For instance, Member States claiming a lawful use of Pegasus for LED purposes should at least prove its compliance with the LED pursuant to Articles 4 and 8 LED.

A notable number of cases on the interpretation of the above provisions is currently pending before the CJEU which should provide for further clarity and legal certainty.

3.1 Introduction

The principles established under Chapter II of the LED are similar to other European and international data protection instruments, yet adapted to the subject matter and aims of the LED. For instance the purpose limitation and data minimisation principles are formulated differently than, for example the GDPR, while the LED also introduces dedicated provisions on storage time-limits, as well as the distinction between different categories of data subject and of data. The adaptation of the data quality principles seeks to accommodate the particular needs of law enforcement and ensure respect not only with personal data protection but also due process.[130] Nevertheless, it should be noted that the LED principles are more flexible than the prominent international instrument on data protection for law

[130] See for example Quezada-Tavárez, K., Vogiatzoglou, P. and Royer, S., 'Legal Challenges in Bringing AI Evidence to the Criminal Courtroom', *New Journal of European Criminal Law*, Vol. 12, No. 4, 2021, pp. 531-551.

enforcement, that is Recommendation 87(15).[131] These differences, according to some scholars, reveal a considerable willingness to loosen obligations for law enforcement authorities.[132] The final draft has also been criticised for not retaining the detailed strict requirements foreseen in the initial LED proposal.[133] It is therefore important to ensure that the LED framework, albeit flexible, does not lead to a lower standard of protection. Of course, Recommendation 87(15) has a guiding nature without the binding power of the LED. Nevertheless, it has been used as a benchmark for setting high standards.[134] In this way, the LED should uphold such standards in the first place, in order for national implementations to follow suit. **In order to avoid the risk of lowering the threshold of protection, the future assessment reports by the European Commission should pay particular attention to the implementation of the data protection principles within the field of criminal justice.**

3.2 Transparency

A notable example of how the LED principles differ from the GDPR counterparts concerns transparency, which is not explicitly foreseen within Article 4. Of course, the nature of criminal justice and law enforcement needs is such as to demand different levels of transparency in order to safeguard criminal investigations and security interests.[135] Nevertheless, a complete absence of the term does not reflect such scaled down function of transparency. The underlying reason and serving purposes are then questionable. The view of the Commission that transparency does not exist in the LED but to some degree is implied within fairness under Article 4(1)(a)[136] seems controversial. WP29 posits that transparency is upheld through the data subject rights under Chapter III of the LED.[137] It has nonetheless been argued that the lack of reference within Article 4 results in transparency and information rights being weaker in the LED.[138] Yet, establishing transparency under Article 4 would not disallow in any way a stricter regulation of data subject rights and provision of broader derogations, as those are justified for security purposes (see also below under section 4). Moreover, the absence of a clear transparency principle possibly conflicts with the European Court of Human Rights (ECtHR) case law.[139] Although transparency overall seems to be enhanced within the LED in comparison to the previous CFD framework, looking forward, its absence amongst the core data protection principles is bound to have an impact.[140]

---

131 Basic Principles of Recommendation No. R (87) 15.

132 De Hert, P. and Papakonstantinou, V., 'The New Police and Criminal Justice Data Protection Directive: A First Analysis', *New Journal of European Criminal Law*, Vol. 7, No. 1, 2016, pp. 7–19.

133 Bäcker, M. and Hornung, G., 'Data Processing by Police and Criminal Justice Authorities in Europe – The Influence of the Commission's Draft on the National Police Laws and Laws of Criminal Procedure', *Computer Law & Security Review*, Vol 28, No. 6, 2012, pp. 627–33.

134 Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70.

135 See also Leiser, M. and Custers, B., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78.

136 Commission Expert Group, Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 November 2016.

137 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 3-6.

138 Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', *Global Privacy Law Review*, Vol. 1, No. 2, 2020, pp. 93–103.

139 Ibid, fn (67) referring to judgment of 6 Sept. 1978, *Klass and Others v. Germany*, App no. 5029/71, para. 36.

140 See also Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340; Leiser, M. and Custers, B., 'The Law

3.3 Purpose limitation

The articulation of the purpose limitation principle and the conditions under which it may be curtailed under Article 4(1) and (2) LED has been subject to criticism for not being sufficiently precise, detailed or practically enforceable.[141] The lengthy debates within academia regarding this provision demonstrates the numerous conceptual problems with which national legal orders have and will be encountered with.

To start with, the reference to purposes set out in Article 1(1) LED is confusing, as the latter defines the scope of the LED in terms of overarching objectives rather than the specified, explicit and legitimate purposes required by the purpose specification principle within Article 4(1).[142] Put differently, the LED does not provide any guidance on how to distinguish between different law enforcement purposes. As described in the CEG fifteenth meeting minutes, the Commission clarified that the objectives under Article 1 are defined in a general manner while purposes have to be specifically defined 'in order to clearly demonstrate what is behind each processing operation and why a certain processing operation is being carried out, such as: identification of a person by using his or her biometric data as a suspect for a crime for the purposes of investigation'.[143] EU data protection bodies have also pointed out that every purpose of processing should be detailed, as 'law enforcement per se, shall not be considered as one specified, explicit and legitimate purpose',[144] and two law enforcement purposes should not be de facto considered compatible because they belong in the same field[145]. Similarly expressed by Advocate General Pitruzzella in his Opinion on a pending case, the mere invocation of a purpose foreseen under Article 1(1) LED is not sufficient to establish that the requirement provided for in Article 4(1)(b) LED is met.[146] The national law regulating an activity pursuing one of the Article 1(1) LED objectives must clearly specify the purposes of the processing.[147] In his view, the lawfulness of the purpose pursued by a processing activity cannot only be established by the mere mention of one of the LED purposes, but it also depends on the circumstances under which it is pursued.[148] It is now up to the Court to provide for further clarity on the interpretation and application of Article 4(1)(b) LED.

Insofar as the second element of the purpose limitation is concerned, that is **the non-incompatibility requirement, it is not explained within the LED whatsoever**. Although the articulation of Article 4(2)

Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78.

141 Jasserand, C., 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?', *European Data Protection Law Review*, Vol. 4, No. 2, 2018, pp. 152–67; Koning, M. E., *The Purpose and Limitations of Purpose Limitation,* Radboud University Nijmegen, Utrecht, Netherlands, 2020; Emanuilov, I., Fantin, S., Marquenie, T. and Vogiatzoglou, P., 'Purpose Limitation By Design as a Counter to Function Creep and System Insecurity in Police AI', *UNICRI Special Collection on AI*, 2020, pp. 26-37.

142 See also Koning, M. E., *The Purpose and Limitations of Purpose Limitation,* Radboud University Nijmegen, Utrecht, Netherlands, 2020.

143 Commission Expert Group, Minutes of the fifteenth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 20 February 2018.

144 Article 29 Data Protection 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 or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015, p. 9.

145 European Data Protection Supervisor, 'Opinion on the Data Protection Reform Package', 12 March 2012, p. 53-54.

146 Opinion of Advocate General Pitruzzella of 30 June 2022, *Ministerstvo na vatreshnite raboti*, C-205/21, ECLI:EU:C:2022:507, paragraph 50.

147 Ibid.

148 Ibid, paragraph 51.

LED resembles its predecessor, Article 3(2) CFD, it has entirely omitted any reference to non-incompatibility, which is by contrast explicitly mentioned as the first condition under Article 3(2)(a) CFD. It has been therefore claimed that Article 4(2) applies regardless of any assessment of compatibility.[149] Another scholar has in fact interpreted Article 4(2) as laying down the rules for incompatible further processing.[150] **Furthermore, the necessity and proportionality test under Article 4(2)(b) LED is arguably less stringent than the respective test under Article 6(4) GDPR, which more clearly echoes the Charter. Be that as it may, compliance with Article 8 of the Charter should in any case be respected and guide the implementation and application of Article 4(2) LED.**[151]

In a recent paper, two scholars have also voiced a contrary opinion, describing Articles 4(1)(b), 4(2) and 4(3) LED as providing for a simpler, more flexible yet highly protective framework.[152] They rely on the Commission's view from the CEG meetings, which posits that the LED does not contain the GDPR concept of further processing, but instead the concept of 'subsequent processing'.[153] In particular, Article 4(2) LED refers to the conditions permitting the *changing* of purpose, that is through authorisation via EU or Member State law and processing that is necessary and proportionate to the new purpose. However, there is little explanation as to what the conceptual difference between further and subsequent processing entails beyond semantics[154], or how this subsequent processing relates to the compatibility requirement[155]. Thereby, the underlying rationale and function of this potentially applicable concept of 'subsequent processing' remains unclear, rendering the argumentation in favour of it rather unconvincing.

Another important issue arising from the ambiguous formulation of Article 4(2) LED relates to the scope of initial processing. In particular, it has been questioned whether Article 4(2) LED applies only to the further processing of personal data initially collected for a law enforcement purpose, under the LED, or

---

[149] Jasserand, C., 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?', *European Data Protection Law Review*, Vol. 4, No. 2, 2018, pp. 152–67.

[150] Koning, M. E., *The Purpose and Limitations of Purpose Limitation,* Radboud University Nijmegen, Utrecht, Netherlands, 2020.

[151] See also Koning, M. E., *The Purpose and Limitations of Purpose Limitation,* Radboud University Nijmegen, Utrecht, Netherlands, 2020.

[152] De Hert, P. and Sajfert, J., 'The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680', Brussels Privacy Hub Working Paper 7, no. 31, December 2021.

[153] Commission Expert Group, Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 November 2016.

[154] De Hert, P. and Sajfert, J., 'The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680', Brussels Privacy Hub Working Paper 7, no. 31, December 2021. In their view, the difference seems to lie on how the GDPR further processing may only take place by the same controller on the same legal basis, while the LED subsequent processing may be undertaken by the same or another controller under the aforementioned Article 4(2) conditions. Nevertheless, this difference seems to reflect to a greater extent how the GDPR and the LED provide for a different framework on lawful processing (six potential legal grounds under Article 6 GDPR versus the one possible legal ground under Article 8 LED), instead of how the purpose limitation principle functions differently yet similarly protectively between these two instruments.

[155] De Hert, P. and Sajfert, J., 'The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680', Brussels Privacy Hub Working Paper 7, no. 31, December 2021.The scholars also mention that subsequent processing and compatibility are 'coupled', but only refer to the example of data transferred by a private entity to a competent authority. An analysis on how Article 4(2) applies to data repurposed within the law enforcement environment is missing.

should also apply to the further processing of personal data initially collected for a GDPR purpose.[156] In other words, after personal data have been transferred under the GDPR to a competent authority, should the processing operation by the competent authority be considered as initial processing under the LED, and thereby subject to Article 4(1)(b), or as further processing within the meaning of Article 4(2), taking into account that the data have been repurposed from the GDPR context? The conditions for processing by the competent authority would differ under Article 4(1)(b) and Article 4(2) LED. However, this is an academic question that did not gain further attention. Instead, it is predominantly perceived that the processing activity in question should be considered as initial processing within the meaning of the LED.[157] Still, **the reference to this academic discussion seeks to demonstrate different aspects of ambiguity arising from Article 4(2) left to be clarified by national laws and practice.**

Nevertheless, the CJEU will also have the opportunity to rule on Article 4(2) LED soon, likely clarifying some of these aspects. More specifically, a Bulgarian administrative court has lodged a request for preliminary ruling on the interpretation of Articles 1(1); 2(1) and (2); 3(1), (2), (7)(a) and (8); 4(2) and 9(1) as implemented into the Bulgarian law transposing the LED.[158] The case concerns the question whether processing personal data of an individual initially categorised as a victim and processing data of the same individual ultimately categorised as an offender (under Article 6, see also below), pursue the same one or two separate purposes. In the Opinion of Advocate General Campos Sánchez-Bordona, the successive attribution of capacities, from victim to offender, constitutes processing under the same purpose of 'investigation' within the meaning of Article 1(1) LED.[159] In this way, the processing purpose is not 'other than that for which the personal data are collected' and thereby Article 4(2) LED is not applicable. As the AG explained, during a criminal investigation, there is a certain fluidity in the categorisation of individuals linked with a crime, until the evidence that emerges leads to a concrete determination of the capacities of the individuals involved.[160]

Moreover, the AG brought forth a systematic or contextual interpretation of Article 4(2) LED, according to which the provision refers to distinct purposes.[161] In other words, it seems that Article 4(2) LED should be applicable when the processing purposes change between the three types of purposes identified under Article 1(1) LED (see above under 2.2). For instance, in this case, Article 4(2) LED would have been applicable if the processing of personal data took place for a different than the 'investigation' purpose. The AG further makes a succinct analysis on how, even if Article 4(2) LED is found to be applicable in this case, its conditions would be very easily met.[162] The CJEU view on the matter will be very welcome.

Article 4(2) is characterised by uncertainty, leaving a wide margin of discretion to Member States, which have to define the conditions for subsequent processing, without any guidance on

---

[156] Jasserand, C., 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?', *European Data Protection Law Review*, Vol. 4, No. 2, 2018, pp. 152–67.

[157] Ibid; De Hert, P. and Sajfert, J., 'The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680', Brussels Privacy Hub Working Paper 7, no. 31, December 2021.

[158] Request for preliminary ruling, *Inspektor v Inspektorata kam Visshia sadeben savet*, C-180/21, 23 March 2021.

[159] Opinion of Advocate General Campos Sánchez-Bordona of 19 May 2022, *Inspektor v Inspektorata kam Visshia sadeben savet*, ECLI:EU:C:2022:406, C-180/21, paragraphs 54, 57, 64.

[160] Ibid, paragraphs 56-57.

[161] Ibid, paragraph 53.

[162] Ibid, paragraphs 65-69.

what constitutes compatible or incompatible purposes pursuant to Article 4(1)(b).[163] The transposition of Article 4(2) LED into national law and its relation to other laws authorising processing for other law enforcement purposes beyond the purposes for which data were initially collected should be further investigated and closely monitored.

Finally, the purpose limitation principle has been on shaking grounds in both GDPR and LED contexts due to numerous challenges in applying it in practice, especially in the environment of big data and AI.[164] Whether specifying purposes within the law, or adhering to the purpose limitation principle on an operational level, authors seem to agree that in order for this principle to work more guidance should be given, or even complementary tools should be adopted, such as impact assessments and the embedding of purpose specification and compatibility considerations in the design of new systems to be used by competent authorities.[165]

3.4 Minimisation, storage limitation and categorisation

Data minimisation

Under Article 4(1)(c) LED, personal data should be 'adequate, relevant and not excessive', instead of 'adequate, relevant and limited to what is necessary', as stipulated under Article 5(1)(c) GDPR. This wording reflects the need for flexibility and for safeguarding criminal procedures, such as an investigation, whereby it is not immediately evident what sort of data are necessary. Some authors have endorsed the Commission's view that this difference in wording indeed allows for more flexibility,[166] as LED controllers can operate with less precision, insofar as they do not process excessive datasets.[167] **It is however not clear how in practice one can easily differentiate between what is not excessive and what is limited to what is necessary.** Moreover, this flexible interpretation of the data minimisation principle could be considered as more liable to abuse. In a similar vein, WP29 in its Opinion on the draft LED Proposal, had insisted that the data minimisation principle includes the phrase 'limited to the minimum necessary'.[168]

---

[163] Jasserand, C., 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?', *European Data Protection Law Review*, Vol. 4, No. 2, 2018, pp. 152–67; Emanuilov, I., Fantin, S., Marquenie, T. and Vogiatzoglou, P., 'Purpose Limitation By Design as a Counter to Function Creep and System Insecurity in Police AI', *UNICRI Special Collection on AI*, 2020, pp. 26-37.

[164] See for example Coudert, F., Dumortier, J. and Verbruggen, F., 'Applying the Purpose Specification Principle in the Age of "Big Data": The Example of Integrated Video Surveillance Platforms in France', ICRI Research Paper 6, 2012, available at https://papers.ssrn.com/abstract=2046123; Moerel, L., and Prins, C., 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things', SSRN Scholarly Paper ID 2784123, 2016, available at https://papers.ssrn.com/abstract=2784123; Emanuilov, I., Fantin, S., Marquenie, T. and Vogiatzoglou, P., 'Purpose Limitation By Design as a Counter to Function Creep and System Insecurity in Police AI', *UNICRI Special Collection on AI*, 2020, pp. 26-37

[165] Ibid.

[166] Commission Expert Group, Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 November 2016.

[167] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873; De Hert, P. and Sajfert, J., 'The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680', Brussels Privacy Hub Working Paper 7, no. 31, December 2021.

[168] Article 29 Data Protection 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 or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015, p. 7.

Nevertheless, in a recent Opinion, Advocate General Pitruzella provided for an interpretation of the data minimisation principle under Article 4(1)(c) LED that seemingly does not differ from that under Article 5(1)(c) GDPR.[169] Accordingly, and with references to ECtHR and CJEU caselaw as well as Recital 26 LED, compliance with the data minimisation principle requires, amongst other, that data are not kept longer than necessary for the purpose pursued and only if the purpose of the processing could not reasonably be fulfilled by other means.[170] Suitability and effective contribution to the fight against crime alone cannot lead to a mentality of maximisation of information which would seriously interfere with fundamental rights. Instead, sufficient safeguards against abuse must be put in place. It will be interesting to see if the Court will adopt such interpretation that does not necessarily distinguish between LED and GDPR.

Time limits for storage and review

A novelty of the LED is the dedicated provision on time limits for storage and a periodic review of the need for storage (Article 5), reinforcing the storage limitation principle within Article 4(1)(e). However, the LED did not go far enough as to provide for concrete criteria regarding the periodic review, nor a clear schedule or methodology for time limits, especially in light of the CJEU case law and the provision of strict storage periods therein.[171] **According to WP29, national laws transposing Article 5 should establish clear and transparent criteria for the assessment of the necessity to further keep personal data, as well as procedural requirements, including the involvement of the Data Protection Officer (DPO)**.[172] Should the controller fail to conduct a periodic review of whether further processing is necessary, then data should be automatically deleted or pseudonymised.[173] The Opinion further argues that Article 5 LED should be read in conjunction with Article 6 LED, and thereby different timeframes should be envisaged for the different categories of data subjects (see also below).

Available sources have documented a variety of time limits across Member States for different situations, including different types of data subjects and different crimes.[174] According to the European Commission report, most national implementing acts only meet the general requirement of Article 5, while sectoral laws must further set limits for erasure or period review.[175] Only a few such sectoral laws seem to exist. In some Member States, it is even left to the competent authority to set such limits, while in some instances the national law does not provide any guidance as to criteria for time limits for storage and period review.

---

169 Opinion of Advocate General Pitruzzella of 30 June 2022, *Ministerstvo na vatreshnite raboti*, C-205/21, ECLI:EU:C:2022:507, paragraphs 54-55.

170 Ibid.

171 Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340. The CJEU case law in question refers to the data retention, access and use periods. Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, C-293/12 and C-594/12, EU:C:2014:238; Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970.

172 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 3-6.

173 Ibid.

174 Leiser, M. and Custers, B., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78.

175 European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 13.

For instance, a scholarly work reports that in Germany, data storage duration is limited depending on the types of persons.[176] The Dutch implementation of the LED foresees that personal data may be stored by the police for one year, a period which can be extended to five years if the data are necessary for the police tasks.[177] However, there are additional different storage and erasure requirements established across different laws that may apply to the same data, often used for different purposes and subject to different rules.[178] Deleting personal data after set time limits seems to be a sensitive topic for law enforcement authorities in the Netherlands. Additionally, Member States sometimes make use of different terms to refer to 'erasure' like 'destruction' or 'removal'.[179] Some national laws transposing the LED, like the Finnish, foresee very precise time durations, while others, like the Irish and Lithuanian, offer significant discretion to the competent authorities themselves, arguably against the wording of the LED.[180]

The CJEU will soon have the opportunity to elucidate the requirements imposed by the storage limitation principle, in response to a request for preliminary ruling by the Bulgarian Supreme Administrative Court.[181] The latter brought into question a national legislative measure, which leads to a virtually unrestricted right of competent authorities to process personal data for LED purposes, and/or to the virtually complete elimination of the data subject's right to restriction and erasure.

Data categorisation

The LED provides for the distinction between different categories of data subjects, as well as between personal data and verification of quality of personal data. While categories of data subjects may include suspects, convicted persons, victims and witnesses,[182] the suggestion by WP29 to include a category of non-suspects subject to more stringent processing and storage conditions was not adopted.[183] **Substantial clarification on these provisions is missing from the LED recitals, with the exception of Recital 31 stipulating that categorisation should not 'prevent the application of the right of presumption of innocence'**. No other safeguard regarding potential consequences of such categorisation upon data subject's rights is defined, potentially allowing for a diverse application of rights corresponding to the different data subject categories.[184]

Categorisation is not a novel concept in EU data protection legislation; the Europol Regulation for instance provides for the assessment of the reliability and quality of the source as well as the accuracy

---

176 Article 35 of Bundesgrenzschutzgesetz 1994, as referred to in an article by Leiser and Custers, ibid.

177 Article 8 of Wet van 21 juli 2007 houdende regels inzake de verwerking van politiegegevens (Wet Politiegegevens, Stb. 2007, 549).

178 Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020, p. 22-27.

179 Ibid, p. 10.

180 Ibid, p. 37; Commission nationale pour la protection des données (Luxembourgish supervisory authority), 'Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7168 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification de certaines lois, Délibération n° 1049/2017 du 28 décembre 2017.

181 Request for preliminary ruling, *NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR*, C-118/22, 17 February 2022.

182 Article 6 of LED.

183 Article 29 Data Protection 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 or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015, p. 7.

184 Cocq, C., 'EU Data Protection Rules Applying to Law Enforcement Activities: Towards an Harmonised Legal Framework?', *New Journal of European Criminal Law*, Vol. 7, No. 3, 2016, pp. 263–76.

of information originating from Member States.[185] However, the LED provisions on categorisation have raised concerns for being static. First, they require complicated decisions to be made on how to typify actors in a crime, at an early stage, while often initial observations may be misguided.[186] Second, criminal investigations are conversely described by fluidity, whereby roles may change over time and evidence on categories builds and updates. Third, roles may overlap or be further spread into sub-categories or a spectrum of involvement in a crime.[187] Fourth, the specifically enumerated data categories are linked to specific time limits that should be equally appointed at an early stage. The LED categorisation provision seems more difficult to adapt in an environment in flux, such as that of criminal investigations, thereby potentially disproportionately affecting certain categories of crime or cold cases.[188] Additionally, the LED categorisation requirement comes on top of pre-existing categories already in place.[189] However, as aforementioned above under 3.3, in a currently pending case before the CJEU, the Opinion of Advocate General Campos Sánchez-Bordona supports a fluid application of Article 6 LED, which does not impact the purpose limitation principle and thereby the lawfulness of processing.[190]

Moreover, another request for preliminary ruling, also on the LED transposition in Bulgaria, will give the CJEU the opportunity to clarify Article 6(a) and whether the categorisation of a data subject as a suspect should be conditional upon the existence of 'serious grounds for believing that they have committed or are about to commit a criminal offence'.[191] In the Opinion of Advocate General Pitruzella, it follows from the letter of Article 6 that it imposes a low intensity and not strictly defined obligation upon Member States, since the list of categories is not exhaustive and the Member States are the ones responsible for determining the consequences of categorisation.[192] Such a literal interpretation allows for a Member State to establish a category of persons against whom accusations have been made, i.e. persons in relation to whom there is sufficient evidence to prove that they have committed a criminal offence.[193] Article 6 LED does not seek to regulate the procedural conditions for the collection of the personal data of persons falling under Article 6(a).[194] The AG concluded that Article 6(a) LED does not preclude national legislation which provides that, if a person, charged with a premeditated criminal offence requiring public prosecution, refused to voluntarily cooperate with the collection of their personal data, the criminal court in charge of authorising a forced collection of said data may do so without needing to assess whether there is sufficient evidence of guilt, since the question of the

[185] Article 29 of 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 ('Europol Regulation') (OJ L 135, 24.5.2016, p. 53).

[186] Leiser, M. and Custers, B., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78; Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020.

[187] Leiser, M. and Custers, B., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78.

[188] Leiser, M. and Custers, B., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78.

[189] Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020.

[190] Opinion of Advocate General Campos Sánchez-Bordona of 19 May 2022, *Inspektor v Inspektorata kam Visshia sadeben savet*, ECLI:EU:C:2022:406, C-180/21, paragraphs 56-63.

[191] Request for a preliminary ruling, *Ministerstvo na vatreshnite raboti v B.C.*, C-205/21, 31 March 2021.

[192] Opinion of Advocate General Pitruzzella of 30 June 2022, *Ministerstvo na vatreshnite raboti*, C-205/21, ECLI:EU:C:2022:507, paragraph 28.

[193] Ibid.

[194] Ibid, paragraph 29.

sufficiency of evidence will be properly presented before the judge, possibly at a later stage of the criminal proceedings.[195]

Finally, distinguishing between facts and mere opinion under Article 7 LED might not be as straightforward either, as there is no clear and objective methodology to that end.[196] Grey zones may include inferred data, such as logical conclusions (inferences on the basis of factual claims) or risk profiles, which do not constitute opinions but rather characteristics derived from data analytics. Statements by victims and witnesses may be unverifiable and subject to challenge during criminal proceedings, while they may contain both fact and opinions.[197]

The practical difficulties faced by law enforcement authorities are also evident in the LED transpositions: Ireland took issue with including possible suspects as a separate category for presumption of innocence reasons, while Denmark admits that this is rarely done in practice due to the circumstances of the case not always being known when the data is recorded, and that it's not always possible to integrate this with their systems.[198] Reports from the Netherlands also confirm how classifying data based on quality is difficult on large scale, and providing categories of data subjects based on their role is cumbersome and 'does not fit police work'.[199] The European Commission report mentions that some national laws do not specify the categories listed in Article 6, while insofar as the 'suspect' category is concerned, the reference to 'serious grounds for believing the persons have committed or are about to commit a criminal offence' under Article 6(a) is omitted.[200] As regards Article 7 LED, the report mentions that it has been transposed by most Member States, although some of its elements are not explicitly required in several national transposing laws.[201]

3.5 Lawful processing under Articles 8-11

General conditions for lawful processing

Article 8 provides the overarching framework for lawful processing; all processing activities must be necessary for the performance of a task carried out by a competent authority for the purposes of the LED and on the basis of EU or national law. Of course, this framework is adapted to the specific needs and functions of competent authorities, whereby GDPR grounds such as consent or contract are inappropriate. Member States enjoy a significant margin of discretion in deciding on grounds for processing, which nevertheless must abide by the Charter.[202]

---

195 Ibid, paragraph 44.

196 Leiser, M. and Custers, B., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78.

197 Ibid.

198 Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020.

199 Ibid.

200 European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 16.

201 Ibid.

202 Bäcker, M. and Hornung, G., 'Data Processing by Police and Criminal Justice Authorities in Europe – The Influence of the Commission's Draft on the National Police Laws and Laws of Criminal Procedure', *Computer Law & Security Review*, Vol 28, No. 6, 2012, pp. 627–33.

In fact, the report by the European Commission mentions that a few national transposing laws refer to consent as a legal basis for processing of personal data, including special categories of data.[203] It further demonstrates how some national laws omitted certain elements from Article 8 LED or did not make explicit the requirement under Article 8(2) LED that the data to be processed and the purposes of processing should be set down in law.[204] The report points out how a mere repetition of Article 8 LED in the national transposing law does not constitute a legal basis; instead, **any law regulating processing by competent authorities must specify which authority is competent to process what personal data for which task and purpose**.[205]

A couple of cases on Article 8 LED have been brought before the CJEU. In its Bundesrepublik Deutschland ruling on processing of personal data by Member States on the basis of a red notice issued by Interpol[206], the Court considered that said processing may be lawful until it has been established in a final judicial decision that the ne bis in idem principle applies in respect of the acts on which that notice is based.[207] Moreover, one of the aforementioned requests for preliminary ruling by a Bulgarian court, also relates to the compatibility of a national law, providing as a general rule for the processing of biometric data of all persons who are charged with a premeditated criminal offence requiring public prosecution, with Articles 8 and 10 LED.[208] Due to its relevance for the conditions on processing of special categories of personal data, the respective Opinion of AG Pitruzzella is discussed below.

Given the rising development and deployment of novel technologies, it is important to examine whether Member States have laws in place regulating their use. A recent report reveals that national legislation on law enforcement might be overly focused on individual cases, specific investigations or persons, thereby not providing in an explicit legal basis or mandate to collect open source intelligence or employ big data tools and AI in law enforcement practice (see also below with regards to automated decision-making).[209] In the Netherlands, for instance, some subject matter experts have suggested that the Dutch legal framework on the processing of police data is insufficiently equipped to properly frame the deployment and adoption of such novel technologies, even though these tools have already been used in practice. As this legislation might lack the necessary details that specify how and by which means certain datasets can be processed, there remains a degree of uncertainty regarding the extent to which the current legal bases might suffice for the collection of

---

[203] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 14.

[204] Ibid.

[205] Ibid.

[206] Judgment of 12 May 2021, *WS v Bundesrepublik Deutschland*, C-505/19, EU:C:2021:376, paragraph 118.

[207] With regards to Interpol and its red notice mechanism, a brief note can be made concerning the misuse of this procedure. In particular, the issuance of red notices leading to arrest can unknowingly be based on politically motivated warrants or court orders and thus result in the violation of the suspect or defendant's human rights. While Interpol itself is not considered a competent authority subject to the LED, national law enforcement agencies and criminal justice authorities are required to adhere to the Directive's principles and standards when following up on red notices and processing personal data in light thereof. In practice, the Bunderepublik Deutschland ruling thus signifies that in the event that it is demonstrated that there do not exist valid grounds for a criminal process against the data subject, the person in question can require Member States to erase the data relating to the red notice. Such a resolution then ought to be communicated to other relevant authorities in order to avoid similar unwarranted arrests elsewhere. For a more extensive examination of this issue and further recommendations in this context, see: Wandall, R., Ensuring the rights of EU citizens against politically motivated Red Notices', European Parliament Committee on Civil Liberties (LIBE), February 2022.

[208] Request for a preliminary ruling, *Ministerstvo na vatreshnite raboti v B.C.*, C-205/21, 31 March 2021.

[209] Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020.

personal data through innovative technological means, as well as for their subsequent use in analytical systems or as training data for AI tools.

Access to personal data collected for non-law enforcement purposes

The 2011 leaked draft version of the LED proposal included a provision regulating access to data initially processed for non-law enforcement purposes.[210] Accordingly, competent authorities would only be able to access such data where specifically authorised by law and where reasonable grounds give reason to consider that the processing will substantial contribute to the pursued purposes, upon written and justified requests and accompanied by appropriate safeguards.

It is also worth mentioning that the European Parliament had suggested to restrict such access for the sole purposes of investigation and prosecution – prevention not included.[211] The rejection of this addition, which would exclude repurposing of data for crime prevention, is considered unfortunate, especially in light of crime prevention technologies being increasingly developed and rolled out amongst Member States, albeit their controversial effectiveness and impact on fundamental rights.

The provision of a framework governing law enforcement access to data collected for other purposes, including data generated within the private sector during commercial activities, would further substantiate the safeguards provided by the CJEU in its respective case law. Accordingly, access to personal data held by ECSPs should be based on objective criteria, whereby a link between the seriousness of crime and the extent of access is established, and access as well as further use are limited to specific persons.[212] The reflection of these safeguards is nonetheless missing from the LED.[213]

The strict requirements for law enforcement access to electronic communications data are all the more important vis-à-vis emerging intrusive hacking technologies such as the Pegasus spyware tool. Pegasus is considered one of the most powerful hacking tools, as it designed to successfully attack almost any smartphone, gaining complete and unrestricted access to it, without requiring any action by the user, while it's also very difficult to detect.[214] Although, the company that developed Pegasus claims it helps prevent and detect serious crimes and terrorist offenses, it has been reported that Pegasus was also used around the world and within the EU to spy on citizens, including journalists, lawyers and politicians.[215]

---

[210] Article 4(2) Proposal for a Directive of the European Parliament and of the Council on the protection of individuals 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 the free movement of such data ("Police and Criminal Justice Data Protection Directive") Version 34 (2011-11-29).

[211] Article 4a of European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals 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 the free movement of such data (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)).

[212] Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, C-293/12 and C-594/12, EU:C:2014:238; Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970.

[213] Jasserand, C., 'Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?', *Computer Law & Security Review*, Vol. 34, No. 1, 2018, pp. 154–65.

[214] Pegg, D. and Cutler, S., 'What is Pegasus spyware and how does it hack phones?', The Guardian, 18 July 2021, available at: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.

[215] European Data Protection Supervisor, Preliminary remarks on modern spyware, 15 February 2022.

In particular, there is a plethora of reports brought together for the European Parliament PEGA Committee which demonstrates how numerous Member States have been involved with Pegasus attacks, either on the attacker's side, the victim's side or both.[216] Accordingly, Hungary, Poland, Spain and Germany have admitted owning and using the software in a lawful, according to these governments, way. France had initiated negotiations to acquire the software which they later interrupted, while Estonia, after acquiring it, was not allowed by Israel and the company itself to use it against Russian targets. Although Bulgaria denies any involvement, it has been reported that one of the servers on which Pegasus' functions rely is located in a Bulgarian datacentre, owned by an NSO Group subsidiary. Greece has been accused of targeting journalists, as well as oppositions politicians, but denies being behind such operations.[217] Hungary and Spain count hundreds of persons targeted by Pegasus, while politicians from Hungary, France, Spain, Finland, Poland, Belgium and the European Commission have also allegedly been victims of Pegasus attacks.

The use of Pegasus constitutes targeted surveillance, which is regulated by national law, as well as it must abide by EU law insofar as it falls within its scope, including the Charter, the EPD and the LED. As mentioned above (see analysis under 2.4 on national security and the LED scope), purely governmental activities in pursuance of national security purposes fall outside the scope of EU law, however they must still meet national and international, including the European Convention on Human Rights (ECHR), requirements against unlawful use.

Besides the questionable uses of Pegasus for national security purposes, all uses 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, certainly fall under the scope of EU law, and thereby must abide by the Charter, EU data protection and other relevant legal frameworks. In his assessment of the compliance of the use of Pegasus with Article 52(1) Charter, the EDPS found that it would likely not reach the necessity and proportionality threshold, while it also affects the essence of the right to privacy.[218] Therefore, the EDPS suggested a ban on the development and the deployment of spyware with the capability of Pegasus in the EU, while he considers that, in case certain features of Pegasus were to be nevertheless applied in exceptional situations, for instance to prevent a very serious imminent threat, a number of steps and measures should be enforced to prevent unlawful use.[219] In that regard, the strict implementation of the EU legal framework on data protection, especially the LED transposition and enforcement, and of the relevant CJEU judgements (e.g. above on data retention) would be of outmost importance.[220]

It is regrettable that the European Commission omitted any mention to the highly questionable use of Pegasus and the effectiveness or lack thereof of the LED against such use. Moreover, the European Commission has decided not to act on all these allegations, claiming that it is a national security issue to be handled by national authorities.[221] Similar claims have been put forth by, for instance, Greece,

---

[216] Marzocchi, O. and Mazzini, M., 'In-Depth Analysis for the Pegasus Committee: Pegasus and Surveillance Spyware', European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, May 2022.

[217] See also Mildebrath, H., 'Greece's Predatorgate: The latest chapter in Europe's spyware scandal?', European Parliamentary Research Service, PE 733.637, September 2022.

[218] European Data Protection Supervisor, Preliminary remarks on modern spyware, 15 February 2022.

[219] Ibid.

[220] Ibid.

[221] Nielsen, N., 'EU Commission won't probe 'Pegasus' spyware abuse', EU Observer, 19 April 2022, available at: https://euobserver.com/digital/154752.

which seeks to regulate the matter internally.[222] Instead, the European Parliament has debated Pegasus in various occasions,[223] and has set up a Committee of Inquiry to investigate the use of the Pegasus and equivalent surveillance spyware.[224] The Committee has further invited Europol to make use of its newly founded powers and assist in the investigations.[225] **Member States claiming a lawful use of Pegasus for LED purposes should at least prove its compliance with the LED, starting with pointing to a legal act clearly indicating the circumstances under which such tools may be used and how such use is necessary for and proportionate to the performance of specific tasks pursuant to Article 8 LED.** Moreover, compliance with other LED provisions analysed throughout this study, such as the data protection principles under this chapter 3, must be further established. Failing to meet these standards, along with fundamental rights and other pertinently relevant legal national constitutional and European frameworks, would result in the lack of lawfulness of the use of such surveillance tools.

Special processing conditions

The LED includes a provision titled 'specific processing conditions', which seems to further elucidate the purpose limitation principle, when personal data transition from the law enforcement to non-law enforcement purposes, that is from the LED to the GDPR or EUDPR framework. Under Article 9(1), personal data initially collected by competent authorities and for law enforcement purposes may only be processed for non-law enforcement purposes if processing is authorised by EU or national law.[226] This clause has become particularly important for conducting research on tools for law enforcement, which often necessitates the use of real data for more efficient designing and testing.[227] Other examples include sharing data with administrative or other public authorities such as tax or customs authorities. One of the pending cases discussed throughout this study concerns amongst other the processing of personal data initially collected in the context of criminal proceedings, then used by the prosecution for the defense in the context of civil proceedings.[228] According to Advocate General Campos Sánchez-Bordona, the lawfulness of said processing must be assessed in light with the GDPR, pursuant to Article 9(1) LED.[229] Article 9(2) further stipulates that the GDPR applies also in the case where competent authorities are entrusted by Member State law with the performance of tasks beyond the scope of the LED, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

---

[222] See e.g. Laura Kabelka, "National security' curtain falls down on Greek spyware scandal investigation', EURACTIVE, 9 September 2022, available at https://www.euractiv.com/section/digital/news/national-security-curtain-falls-down-on-greek-spyware-scandal-investigation/.

[223] Marzocchi, O. and Mazzini, M., 'In-Depth Analysis for the Pegasus Committee: Pegasus and Surveillance Spyware', European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, May 2022.

[224] For more information, see website of PEGA Committee at https://www.europarl.europa.eu/committees/en/pega/home/highlights.

[225] Lenaers, J. Chair of Committee of Inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, 'Request from PEGA Committee on Europol use of its new power under Regulation (EU) 2022/991, 28 September 2022.

[226] Article 9(1) of LED.

[227] Bolognini, L., A Proposal for the EU Privacy Law Simplification, Supporting Data-Driven Research in the Law Enforcement Field', Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP), 10 January 2020, available at https://www.istitutoitalianoprivacy.it/2020/01/10/a-proposal-for-the-eu-law-simplification-supporting-data-driven-research-in-the-law-enforcement-field/; H2020 VICTORIA – Grant Agreement No 740754, 'VICTORIA Policy Guidelines', D3.3 Report on the Implementation of VICTORIA Ethical and Legal Guidelines, April 2020, H2020 MAGNETO – Grant Agreement No 786629, D9.4 Final Ethical and Legal Assessment, April 2021.

[228] Request for preliminary ruling, *Inspektor v Inspektorata kam Visshia sadeben savet*, C-180/21, 23 March 2021.

[229] Opinion of Advocate General Campos Sánchez-Bordona of 19 May 2022, *Inspektor v Inspektorata kam Visshia sadeben savet*, ECLI:EU:C:2022:406, C-180/21, 85.

As explained by Recital 34 LED, '[f]or the processing of personal data by a recipient that is not a competent authority or that is not acting as such within the meaning of this Directive and to which personal data are lawfully disclosed by a competent authority, the [GDPR] should apply. While implementing the [LED], Member States should also be able to further specify the application of the rules of the [GDPR], subject to the conditions set out therein.' In principle, triggering the GDPR means that its principles and rules such as information obligations and data subject rights as established in the GDPR should apply. **Therefore, the conditions under which personal data collected by competent authorities may be further processed by the competent authorities themselves or by other entities for non-law enforcement purposes depends on the transposition of the LED in each Member State.** Currently, we can observe a lack of (clear and foreseeable) legislative framework on both EU and national levels.[230]

Especially in the context of scientific research which may heavily rely on criminal data, scholars have formulated recommendations to provide for further guidance or such legal authorisation under Article 9(1),[231] or even to amend said provision[232].

Finally, Article 9(3) provides for the possibility to apply specific conditions in specific circumstances when personal data are transmitted, such as the use of handling codes according to Recital (34). The latter further clarifies that such specific conditions may include a prohibition against further transmission or further processing for other purposes. However, in accordance with Article 9(4), such specific conditions should not differ than those applicable to similar data transmissions within the Member State of the transmitting competent authority. Respectively, such Member State-set specific processing conditions should be respected by AFSJ agencies, offices and bodies, pursuant to Article 75 of the EUDPR.

Processing of special categories of personal data

The LED does not prohibit processing of special categories of personal data per se, as opposed to the GDPR[233] and the EDPS and WP29 recommendations on the draft LED[234], but this is allowed only where strictly necessary, subject to appropriate safeguards, and if one of the three conditions foreseen under Article 10 apply. This reversal of phrasing, from prohibition to permission under conditions albeit strict,

---

[230] See for example Bolognini, L., A Proposal for the EU Privacy Law Simplification, Supporting Data-Driven Research in the Law Enforcement Field', Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP), 10 January 2020, available at https://www.istitutoitalianoprivacy.it/2020/01/10/a-proposal-for-the-eu-law-simplification-supporting-data-driven-research-in-the-law-enforcement-field/; H2020 VICTORIA – Grant Agreement No 740754, 'VICTORIA Policy Guidelines', D3.3 Report on the Implementation of VICTORIA Ethical and Legal Guidelines, April 2020, H2020 MAGNETO – Grant Agreement No 786629, D9.4 Final Ethical and Legal Assessment, April 2021; De Hert, P. and Sajfert, J., 'The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680', Brussels Privacy Hub Working Paper 7, no. 31, December 2021.

[231] See for example H2020 VICTORIA – Grant Agreement No 740754, 'VICTORIA Policy Guidelines', D3.3 Report on the Implementation of VICTORIA Ethical and Legal Guidelines, April 2020, H2020 MAGNETO – Grant Agreement No 786629, D9.4 Final Ethical and Legal Assessment, April 2021.

[232] Bolognini, L., A Proposal for the EU Privacy Law Simplification, Supporting Data-Driven Research in the Law Enforcement Field', Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP), 10 January 2020, available at https://www.istitutoitalianoprivacy.it/2020/01/10/a-proposal-for-the-eu-law-simplification-supporting-data-driven-research-in-the-law-enforcement-field/;

[233] Article 9(1) of GDPR.

[234] European Data Protection Supervisor, Opinion 6/2015, 28 October 2015, p. 6; Article 29 Data Protection 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 or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015, p. 8.

has raised concerns about endangering data subjects' rights and alarmingly lowering the level of protection.[235]

Pursuant to dominant understanding, Article 10 functions complementary to the Article 8 general conditions for lawful processing. More specifically, the European Commission, in response to questions from Member States during the 9th CEG meeting, clarified that '[t]he relationship between Article 8 and 10 means that processing of special categories of data always have to be provided for by law, and in addition it is allowed only when strictly necessary and subject to appropriate safeguards, also laid down in law'.[236] Similarly, WP29 opined that Articles 10 and 8 are interrelated; the grounds under Article 10(a)-(c) merely illustrate specific situations under which processing of special categories of personal data may be considered as strictly necessary.[237] Literature seems to agree as well, considering the elements under Article 10 of 'strictly necessary' and 'appropriate safeguards' as the two additional requirements alongside the general lawfulness requirements of Article 8.[238]

While promoting a higher protective framework, these interpretations are not necessarily coherent with the wording of the LED itself, which foresees two potential situations whereby having a basis in the law does not seem to be a prerequisite under Article 10(b)-(c). They also seem to contradict Recital 37 stipulating that '[s]uch [special categories of] personal data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; where not already authorised by such a law, the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject.'[239] Alternatively, 'authorised' under Article 10 should be read as implying a separate, perhaps more explicit, reference within the law, in comparison to 'based' under Article 8.

Insomuch as this interpretation is dominant, and allows for a reinforced level of protection for data subjects, it seems reasonable to assume that it should be followed by Member States as well. In that case, processing of special categories of personal data is allowed only where it is strictly necessary for the performance of a law enforcement task based on EU or national law, it is subject to appropriate safeguards, and where one the following applies: it is further authorised by EU or national law, or it aims to protect a person's vital interests, or data are manifestly made public by the data subject. In the Opinion by Advocate General Pitruzzella, it is noted that the Spanish, German, English, Polish, Portuguese and Romanian languages, the phrasing of Article 10 is different, referring not to the French 'absolutely necessary (absolument nécessaire)' but to 'strictly necessary (strictement nécessaire)'[240], which could further complicate a comprehensive application of the provision amongst Member State. Nevertheless, the AG considers this subtle difference in wording to be non-consequential with regards to the heightened level of necessity that this provision requires, given the sensitive nature of the data

[235] Cocq, C., 'EU Data Protection Rules Applying to Law Enforcement Activities: Towards an Harmonised Legal Framework?', *New Journal of European Criminal Law*, Vol. 7, No. 3, 2016, pp. 263–76.

[236] Commission Expert Group, Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4 May 2017.

[237] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 7.

[238] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

[239] By contrast, Recital 51 of GDPR explicitly states that the Article 9 on processing of special categories of personal data provides for the specific requirements for such processing, while 'the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing'.

[240] Opinion of Advocate General Pitruzzella of 30 June 2022, *Ministerstvo na vatreshnite raboti*, C-205/21, ECLI:EU:C:2022:507, paragraph 49.

in question. With regards to the condition that data are manifestly made public by the data subject, WP29 recommends that 'data manifestly made public' should be interpreted narrowly, taking into account the reasonable expectations of the data subject.[241]

A decisive ruling may soon be provided by the CJEU in the pending case from Bulgaria regarding forced collection of data and the processing of biometric and genetic data of all persons charged with a premeditated criminal offence requiring public prosecution.[242] In his Opinion, Advocate General Pitruzzella confirmed that Article 10 LED is a specific provision on processing of special categories of personal data which does not prejudice the application of the rest LED provisions, including Articles 4(1) and 8 LED.[243] Having said that, the AG regrettably considered the successive examination of all these provisions as redundant and focused only on the conditions of Article 10 LED.[244] Accordingly, first, the examination of strict necessity under Article 10 relates primarily to the principles of purpose limitation and data minimisation (see discussions above under 3.3 and 3.4).[245] In that regard, the AG points to previous caselaw, according to which only the fight against serious crime and safeguarding of public security may justify serious interferences with fundamental rights.[246] In this way, processing of special categories of personal data may only be justified, in his view, by objectives related to the fight against serious crime.[247] This line of reasoning, if adopted by the Court, would need further elaboration.

Second, the condition of authorisation by Member State law under Article 10(a) LED which is most relevant for the case in question, requires that the national law meets the requirements under Recital 33.[248] More specifically, the law must specify both the general objectives and the purposes in a way that the direct relevance of the envisaged processing is clear. Third, insofar as the appropriate safeguards are concerned, they must be foreseen in the national law, which should provide a clear picture of the envisaged processing in order for abusive processing to be avoided.[249] Examples of safeguards are provided under Recital 37, while for special categories of personal data the issues for storage duration and access by competent authorities are of crucial importance. The AG concludes with a highly strict set of conditions that a national law authorising the processing of special categories of personal data by competent authorities should fulfil, including the specification of precise purposes, the necessity of the processing of the specific special category of personal data and the conditions of processing throughout the entire lifecycle of the data.[250] It remains to be seen whether the CJEU will endorse this approach, and whether Member State laws can and do actually meet these requirements. On the basis of the information provided during the proceedings, the AG is doubtful of the compatibility of Bulgarian law, imposing the processing of biometric and genetic data of all all persons who are charged with a premeditated criminal offence requiring public prosecution, with Article 10 LED.[251]

---

241 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 10.

242 Request for a preliminary ruling, *Ministerstvo na vatreshnite raboti v B.C.*, C-205/21, 31 March 2021.

243 Opinion of Advocate General Pitruzzella of 30 June 2022, *Ministerstvo na vatreshnite raboti*, C-205/21, ECLI:EU:C:2022:507, paragraph 46.

244 Ibid, paragraph 47.

245 Ibid, paragraphs 49-55.

246 Ibid, paragraph 50.

247 Ibid, paragraph 50.

248 Ibid, paragraph 56.

249 Ibid, paragraph 57.

250 Ibid, paragraph 58.

251 Ibid, paragraphs 59-64.

It must therefore be examined in a targeted manner whether Member States have applied these provisions coherently. It is important to collect information on national laws providing for the legal basis for the processing of special categories of personal data, which may concern standard procedures like taking of fingerprints, or the use of advanced algorithmic tools, such as facial recognition.[252] In that respect, a report on facial recognition documents how in France not any law but a decree from the Conseil d'État is required for the processing of special categories of personal data by the State, while in Sweden special categories of data processing by competent authorities is only allowed when it is absolutely necessary for law enforcement purposes.[253] The analysis demonstrates an absence at the time when the report was drafted, of dedicated national legislations providing a specific framework for the deployment of facial recognition technologies.[254] The proposed AI Act foresees the prohibition of 'real-time' remote biometric identification systems in publicly accessible spaces employed by law enforcement.[255] However, major exceptions to this prohibition are provided[256], while calls for a wider prohibition on facial recognition have also been made[257].

The report by the European Commission documents how most (and regrettably not all) Member States make reference to strict necessity as a prerequisite for processing of special categories of personal data.[258] Most national laws also provide for the same three alternative conditions under Article 10(a)-(c) LED, while some include additional grounds relating to the protection of human life.[259]

Finally, with respect to appropriate safeguards, although Recital 37 provides several examples, including stricter rules on access and prohibition of transmission, **the LED does not foresee any safeguards for minors.** This shortcoming was also pointed out by the Greek supervisory authority with regards to the Greek transposition of the LED.[260] Given the particularly vulnerable position of minors and the emerging roll-out of technologies targeting youth delinquency[261], formulating tailored safeguards is essential.

---

[252] See also Chairman of Committee on Civil Liberties, Justice and Home Affairs, 'LIBE Contribution to the Commission upcoming report on the evaluation and review of the Law Enforcement Directive', IPOL-COM-LIBE D (2022)3535, 7 February 2022.

[253] Lequesne Roth, C., Kimri, M., and Legros, P., 'La Reconnaissance Faciale dans l'espace public – Une cartographie européenne', [Rapport de recherche] Université Côte d'Azur, Nice, France, 2020, ffhal-03133123f.

[254] Ibid.

[255] Article 5(1)(d) of Proposed AI Act.

[256] Article 5(1)(d), (2)-(4) of Proposed AI Act.

[257] European Data Protection Supervisor, Press Release Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary, EDPS/2021/09, 23 April 2021; EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021.

[258] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 14.

[259] Ibid.

[260] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Greek supervisory authority), Γνωμοδότηση 1/2020, Athens 24 January 2020.

[261] See for example predictive policing technologies in the Netherlands, including systems that target minors: Amnesty International, 'We Sense Trouble – Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands', 2020, available at https://www.amnesty.nl/content/uploads/2020/09/Report-Predictive-Policing-RM-7.0-FINAL-TEXT_CK-2.pdf?x62320

Automated individual decision-making, including profiling

Whereas in the GDPR the framework on automated decision-making is foreseen as part of the data subject's rights[262], the LED regulates automated decision-making in Chapter II Principles. The introduction of a prohibition of automated decision-making in law enforcement and criminal justice has been welcomed. At the same time, scholars have questioned the adequacy of Article 11 to establish a highly protective framework for data subjects, in light of technological trends.[263] The prohibition may be simply lifted by virtue of EU or Member State law, and thereby its impact depends on the foreseen conditions. Insofar as Article 11 LED echoes Article 22 GDPR, the same abundantly discussed limitations apply, while the LED framework on automated decision-making is considered significantly weaker than the one provided by the GDPR[264]. In that regard, the absence of specific guidelines on an EU level on such an impactful provision is regrettable.[265]

To start with, the prohibition on automated decision-making information is focused on individual decision-making, setting aside collective or group profiling. This may be problematic in several areas, including predictive policing technologies, for instance, which identify crime hotspots thereby making it difficult to discern whether it is the individual or the group of residents of an area that is affected.[266]

Moreover, as Article 11 is limited to 'decision-making solely based on automated means', scholars have questioned what constitutes a decision, what is the extent and nature of human intervention required[267], and whether any '*preliminary* profiling' (emphasis in original text) would be covered[268]. For instance, the UK developed 'Harm Assessment Risk Tool' (HART) which provides recommendations on offenders' rehabilitation prospects may not consist of a solely automated decision and thereby fall outside the scope of Article 11.[269] Another example given relates to the creation by the Italian Lombardy region of a mapping of Roma population[270] to be potentially used for prosecutorial purposes, which could fall outside the scope of Article 11, as it may be considered as preliminary profiling and not a decision solely based on automated means.[271] Decision-making processed with multiple stages, potentially comprising of both manual and automated means, could escape the

[262] Article 22 of GDPR.

[263] Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340; Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873; Lynskey, O., 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' *International Journal of Law in Context*, Vol. 15, No. 2, 2019, pp. 162–76.

[264] González Fuster, G., 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights', European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 656.295, 2020.

[265] Ibid.

[266] Lynskey, O., 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' *International Journal of Law in Context*, Vol. 15, No. 2, 2019, pp. 162–76.

[267] Ibid.

[268] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

[269] Lynskey, O., 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' *International Journal of Law in Context*, Vol. 15, No. 2, 2019, pp. 162–76. See also Oswald M., Grace, J., Urwin, S. and Barnes, G., 'Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality', *Information & Communications Technology Law*, Vol. 27, No. 2, 2018, pp. 223–50.

[270] Decision of the Lombardy Regional Council NOXI/40 of 3 July 2018, also reported in La Stampa, available at http://www.lastampa.it/2018/07/04/esteri/lombardy-moves-forward-with-roma-census-DoA54EOBA3srT6LE3d1IVO/pagina.html.

[271] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

stricter regime of Article 11.[272] Additionally, there exists the risk that a simple act of confirming a computer-generated decision by an officer will be considered as human intervention and thereby the decision will not be considered as based solely on automated means. The right to obtain human intervention is in essence minimal, as it does not need to be anything more than nominal; in other words, any human intervention would suffice, while a substantial, reasoned scrutiny is not foreseen.[273] Automated decisions, including profiling, that do not fall within the scope of the Article 11 LED prohibition, must still abide by the general framework for all types of data processing provided by the LED. Nevertheless, the issues highlighted above demonstrate how applying Article 11 may be anything but straightforward, while potentially risky systems could evade stricter regulation.

It should also be noted that, while profiling resulting in discrimination on the basis of special categories of personal data processing is prohibited, the extent to which this provision covers indirect, and potentially less provable, discrimination, is debateable.[274] Additionally, as special categories of personal data, albeit similar to discrimination grounds under EU discrimination law, are listed in an exhaustive manner, this provision might not cover criminal profiling by emerging technologies resulting in new forms of unfair differentiation on the basis of other types of data.[275]

Furthermore, what constitutes an adverse legal or significant effect under Article 11(1) is left undefined, while the choice of slightly different wording between Article 11 LED and Article 22 GDPR is not explained nor substantiated[276]. Similarly, the reference to 'suitable measures to safeguard a data subject's rights and freedoms and legitimate interests' under Article 11(2) is awfully vague.[277] Examples of 'appropriate safeguards' under Article 11(1), which seemingly differ from the aforementioned suitable measures, are only given in Recital 38. Accordingly, suitable safeguards include 'the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision'. Given the non-binding nature of recitals, however, individuals may never be informed about being subject to automated decision-making or profiling, as providing this information is not explicitly required within the provisions of the LED, specifically under Chapter III, as also discussed in section 4.[278]

---

[272] Binns, R. and Veale, M., 'Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR' *International Data Privacy Law*, Vol. 11, No. 4, 2021.

[273] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

[274] Lynskey, O., 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' *International Journal of Law in Context*, Vol. 15, No. 2, 2019, pp. 162–76.

[275] Naudts, L., 'Criminal Profiling and Non-Discrimination: On Firm Grounds for the Digital Era?', *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructures*, Vedder, A. et al. (eds), 1st ed., KU Leuven Centre for IT & IP Law Series 7, Intersentia, Cambridge, Antwerp, Chicago, 2019, pp. 63–96.

[276] Article 11 of LED makes reference to '*adverse* legal effect' and '*significantly* affect', whereas Article 22 of GDPR refers to 'legal effects' and '*similarly* significantly affect'.

[277] Lynskey, O., 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' *International Journal of Law in Context*, Vol. 15, No. 2, 2019, pp. 162–76; Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340.

[278] Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' Privacy Technologies and Policy, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30; Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', Global Privacy Law Review, Vol. 1, No. 2, 2020, pp. 93–103; González Fuster, G., 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights', European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 656.295, 2020.

Thereby, the impact of Article 11 will depend on national transpositions, while its applicability in the law enforcement environment allows higher degrees of discretion to controllers.[279] In that regard, WP29 recommended that national legislators place an obligation upon controllers to carry out a Data Protection Impact Assessment (DPIA) in connection with automated decisions.[280] Finally, information and even more so explanation on automated decision-making may be hampered by legal restraints such as the protection of the algorithms in question by trade secrets or intellectual property rights.

Insofar as automated decision making is concerned, the proposed AI Act could potentially have a significant impact on use of AI systems by criminal justice actors. First, as aforementioned (under 2.5), the EDPB and EDPS as well as the IMCO and LIBE Committees of the European Parliament have called for the prohibition of predictive policing against individuals.[281] Second, the proposed AI Act provides for a set of requirements for high risk AI systems[282], including a risk management system, transparency, and human oversight. Providers of such AI systems must demonstrate the conformity with said requirements before the system enters the market. As explained in Article 14(2) of the proposed AI Act, '[h]uman oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights'. It should include measures to fully understand, interpret and even disregard or override the AI system's output.[283] In this way, the proposed AI Act requirements should facilitate the implementation of Article 11 LED, by rendering solely automated decisions more explainable to and debatable by its user. However, criticism has been raised on how the proposed AI Act fails to impose specific mechanisms at specific stages to effectively implement transparency and human oversight.[284] It also addresses primarily the providers of AI systems, without providing for direct oversight obligations upon the user, in this case an LED competent authority, who enjoy a wider discretion.[285] Moreover, transparency is not required to be provided to the individual(s) affected by an AI system, while the transparency obligation is regrettably not applicable to AI systems 'authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence'.[286] In their joint opinion, the EDPB and EDPS criticised this exception for being too broad, while they also called for 'new, more proactive and timely ways to inform users of AI systems on the (decision-making) status where the system lays at any time, providing early warning of

[279] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873; González Fuster, G., 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights', European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 656.295, 2020.

[280] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 15.

[281] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021; European Parliament, Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, 2021/0106(COD), 20 April 2022.

[282] Title III, Chapter 2 of Proposed AI Act.

[283] Article 14 of Proposed AI Act.

[284] Ebers M. et al., 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)', J Vol. 4, No. 4, 2021, pp. 589–603; Trilateral Research, 'Human intervention and human oversight in the GDPR and AI Act', available at: https://trilateralresearch.com/research-highlights/human-intervetion-in-gdpr-and-ai.

[285] Article 29 of Proposed AI Act.

[286] Article 52(1) of Proposed AI Act.

potential harmful outcomes'.[287] As aforementioned, given that the proposed AI Act is currently under the legislative process, with a substantial amendments being proposed, there is room for the final text to ensure a streamlined with the LED and overarchingly strong framework of protection for AI systems used within criminal justice (and beyond).

Consequently, maintaining a high level of protection for the rights and freedoms of data subjects will depend on EU and national laws authorising automated decision-making and the safeguards stipulated therein. The gaps identified within Article 11 will have to be addressed, if so, on a case-by-case basis.

In that regard, the transposition of Article 11 amongst Member States has received some attention. In the Austrian transposition of the LED, the prohibition of automated decision-making is articulated similarly to Article 11 LED but with less explicit reference to safeguards, while profiling based on special categories of data is allowed unless it is not objectively justified.[288] Similarly, the wording chosen by the German legislator resounds the LED, but is more broadly articulated than Article 11(1), while an express reference to processing of special categories of personal data is omitted throughout the provision.[289] Ireland opted for a reservation clause, in the sense that the provision on automated decision-making does not apply unless certain requirements are met. Although there too no express reference to processing of special categories of personal data is made, a ban of discrimination is foreseen.[290] Whereas the Finnish law prohibits automated decision-making only when it results in discrimination, it also makes numerous references to the importance of human rights and highlights how the police should choose the most appropriate avenues to minimize interferences with human rights.[291] The Netherlands have adopted an unclear interpretation of automated decision-making in the law transposing the LED, which is not sufficiently prepared to deal with processing operations through new technologies.[292] Shortcomings relate, for example, to the existence of a legal basis, and the conditions for using personal data for specific tools, as well as for training new technologies. This seems to create a loophole whereby more activities are taking place than actually allowed by law.

As noted in the European Commission report, while most national transposing laws require that the existence for suitable safeguards for automated decisions based on sensitive data, and prohibit profiling that results in discrimination, not all Member States foresee the right to obtain human intervention or require suitable measures to safeguard data subject's rights, freedoms and interests.[293]

---

[287] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021.

[288] Hudobnik, M., 'Data Protection and the Law Enforcement Directive: A Procrustean Bed across Europe?', *ERA Forum*, Vol. 21, No. 3, 2020, pp. 485–500.

[289] Ibid.

[290] Ibid.

[291] Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020, p. 120.

[292] Ibid, p. 24, 27.

[293] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 14-15.

4. RIGHTS OF THE DATA SUBJECT

KEY FINDINGS

Concerns have been raised in respect to Article 13, the information requirements therein, and the absence of a notification duty in line with European case law. Ambiguity has been reported regarding the right to restriction, which should be implemented by Member States as a distinct right.

Although a restriction of rights should be counter-balanced through the possibility of indirect exercise of rights by the supervisory authority, theoretical and practical difficulties have been pointed out. Additionally, Article 17 has been erroneously transposed in a few Member States. As Article 18 significantly limits data subject's rights allowing for national divergencies, a detailed overview of the transposition of Chapter III within Member States, including federal regimes and national criminal procedural law provisions, should be provided.

The LED offers a wide discretionary power to Member States when it comes to data subject's rights, and reports on national transposition paint a troubling picture; more effort should be put both in providing information and in handling data subject's rights requests.

While further guidance on the modalities for exercising data subject's rights from national and European bodies is encouraged, recent reports do show a heightened awareness on data protection within criminal justice.

4.1 Introduction

The importance of data subject's rights, particularly the right of access which is considered a prerequisite for the exercise of all other rights, is abundantly documented in literature and jurisprudence.[294] The rights of access and rectification are also guaranteed within the fundamental right to personal data protection under Article 8(2) of the Charter. Data subject's rights empower the individual with control over their personal data, and enhance accountability, lawful processing and transparency, which, as mentioned, is not explicitly stipulated within the LED. They thereby comprise an essential tool against informational power asymmetries and unlawful processing operations. The LED provisions governing the exercise of data subject's rights are also relevant for other legal instruments, such as the PNR Directive which designates the CFD as the applicable framework for the protection of personal data.[295]

[294] See for example Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' *Privacy Technologies and Policy*, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30 Vogiatzoglou, P., Quezada Tavárez, K., Fantin, S. and Dewitte, P., 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives', *Journal of Intellectual Property, Information Technology and E-Commerce Law,* Vol. 11, No 3, 2020, pp. 274–302; Quezada Tavárez, K., 'Impact of the Right of Access on the Balance between Security and Fundamental Right: Informational Power as a Tool to Watch the Watchers', *European Data Protection Law Review*, Vol. 7, No. 1, 2021, pp. 59–73. On CJEU case law see amongst other Judgment of 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer,* C-553/07, EU:C:2009:293, paragraphs 51-52; Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner,* C-434/16, EU:C:2017:994, paragraph 57.

[295] Article 13 of PNR Directive.

Obviously, data subject's rights in the LED are adapted to the criminal justice domain, whereby certain limitations must apply to safeguard security and criminal investigations. Nonetheless, a right balance between security interests and individuals' rights and freedoms must be struck. As noted by WP29, **the LED does not allow for blanket restrictions to data subject rights; instead, restrictions should only be possible where they constitute a necessary and proportionate measure and interpreted in a restrictive manner**.[296] It is therefore crucial to investigate whether a balance between the conflicting interests has been struck both in the LED and in the national implementing acts.

4.2 Information to be made available and rights

Article 13 lays down the sets of information to be made available to the data subject in general under Alinea (1), as well as in specific cases under Alinea (2), unless the conditions of Alinea (3) apply. It is not clear, however, what these 'specific cases' may refer to. According to WP29 'it can be argued that this duty does not relate to a certain data subject, but to a certain processing procedure and all data subjects potentially affected by it'.[297] Further on in their Opinion, it is mentioned that specific cases may concern situations where data are collected either directly from the data subject or indirectly without their knowledge.[298] It is questionable though, whether Article 13(2) refers to a proactive action or an ex post right of access, while both views have been supports within literature.[299] **A number of ambiguities surrounding Article 13(2) are thereby left upon Member States to clarify.** Moreover, as the provision of information under Article 13(2) may be delayed, restricted or omitted on the basis of national laws, WP29 recommended that objective criteria be defined therein to that end.[300] As noted elsewhere, excluding information for longer periods or even permanently in order, for example, for the data subject not to be able to draw conclusions as to the modus operandi of the authority would be disproportionate.[301]

A question that has been raised within the legal literature is to what extent Article 13 may be assimilated with the right to notification as developed with European jurisprudence.[302] In particular, pursuant to the CJEU Tele2 Sverige ruling, individuals whose personal data are processed, and are thereby affected, must be notified 'under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to

[296] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 24.

[297] Ibid, p. 17.

[298] Ibid, p. 18.

[299] Sajert and Quintel consider Article 13(2) as providing for a scenario whereby the competent authority proactively decides to provide information, while Vogiatzoglou et al consider it a complementary ex post right of access. Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873; Vogiatzoglou, P., Quezada Tavárez, K., Fantin, S. and Dewitte, P., 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives', *Journal of Intellectual Property, Information Technology and E-Commerce Law,* Vol. 11, No 3, 2020, pp. 274–302.

[300] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 18.

[301] Bäcker, M. and Hornung, G., 'Data Processing by Police and Criminal Justice Authorities in Europe – The Influence of the Commission's Draft on the National Police Laws and Laws of Criminal Procedure', *Computer Law & Security Review*, Vol 28, No. 6, 2012, pp. 627–33.

[302] Ibid, Jasserand, C., 'Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?', Computer Law & Security Review, Vol. 34, No. 1, 2018, pp. 154–65.

a legal remedy'.[303] The ECtHR[304] and Recommendation R(87) 15[305] similarly highlight the importance of notifying individuals with respect to processing operations that affect them, in order for them to be able to seek effective remedy, as soon as the police operations are no longer jeopardised. Therefore, even though the abovementioned Tele2 Sverige ruling by the CJEU was only published after the adoption of the LED, the right to notification was well established within the European legal order and could have been taken into account within the LED. **Nevertheless, the information requirements under Article 13 do not reflect such notification duty.**[306]

Insofar as the information stipulated under Article 13 to be made available and even more so the right of access under Article 14 are concerned, certain limitations have been pointed out.[307] Neither Article 13 nor Article 14 foresee that information regarding automated decision-making, including profiling is to be provided[308], although this gap could perhaps be remedied by virtue of Article 11 in combination with Recital 38, as discussed above. No explicit reference is made to joint controllership, as further explained in section 5. Where data have been transferred to third countries or international organisations, the provision of information under Article 13may be limited to categories of recipients rather than a specific list, while information on appropriate safeguards adopted is not required. Additionally, the definition of 'recipient' under Article 3(10) excludes public authorities which receive data in the framework of a particular inquiry in accordance with Union or Member State law, such as for instance tax and customs authorities. Thereby data subjects may not be informed of their data being transmitted to said authorities. Recital 43 also demonstrates how information does not need to be detailed or include an actual copy of the data processed; instead a full summary is sufficient. Finally, safeguards are also only stipulated within the non-binding Recitals, for instance that any restriction of the right of access should be assessed individually, and comply with the Charter and the ECHR.[309]

Next to the right to access, the LED provides for the right to rectification, to erasure, and to restriction as an alternative to erasure. Although not foreseen as an independent right in Article 16, WP29 has posited that a right to restriction should exist separately from the right to erasure, as distinctly

---

[303] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 121.

[304] Accordingly, 'notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned.' See for example Weber and Saravia v. Germany, App. no. 54934/00, 29 June 2006, paragraph 135; Roman Zakharov v. Russia, App. no. 47143/06, 11 December 2015, paragraph 287; Szabó and Vissy v. Hungary, App. no. 37138/14, 12 January 2016, paragraph 86.

[305] Principle 2.2 of Council of Europe, Committee of Ministers, Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, 17 September 1987.

[306] Jasserand, C., 'Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?', Computer Law & Security Review, Vol. 34, No. 1, 2018, pp. 154–65. See also Bäcker, M. and Hornung, G., 'Data Processing by Police and Criminal Justice Authorities in Europe – The Influence of the Commission's Draft on the National Police Laws and Laws of Criminal Procedure', *Computer Law & Security Review*, Vol 28, No. 6, 2012, pp. 627–33.

[307] Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' Privacy Technologies and Policy, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30; Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', Global Privacy Law Review, Vol. 1, No. 2, 2020, pp. 93–103; González Fuster, G., 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights', European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 656.295, 2020.

[308] Ibid. See by contrast Articles 13(2)(f), 14(2)(g) and 15(1)(h) of GDPR.

[309] Recitals 44 and 46 of LED.

stipulated in Recitals 47 and 48.[310] In particular, while Article 16(3) articulates an obligation of the controller to restrict processing, Recitals 47 and 48 refer to the right to restriction. **Given this ambiguity, it should be investigated whether Member States lay down such a right to restriction in their national legislation, both as a corollary to the right of erasure and as a distinct right.** Regrettably, there is no equivalent right to object under the LED.[311]

The right of access may be partly or even wholly restricted in line with Article 15, while information requirements and the rights to rectification, erasure or restriction may equally be restricted for the same reasons.[312] The foreseen restriction grounds are articulated in broad terms, potentially allowing Member States to provide controllers with a wide discretionary power in refusing to comply with data subject's rights.[313] Apart from the grounds outlined therein, Member States may also adopt legislative measures determining specific categories of processing activities whereby the right of access may be wholly or partly restricted.[314] Albeit justifiable for reasons of security and to safeguard the integrity of criminal investigations, the complete restriction of the right of access should be counterbalanced. Instead of an ex ante notification obligation, as discussed above, a review by the supervisory authority is foreseen, as detailed below, under Article 17. Additionally, as advocated above by WP29, any restriction of data subject's rights should not be blanket nor perpetual.

Granting a direct right of access denotes a significant progress from the previous situation under the CFD.[315] Further welcomed safeguards include the protection of confidential sources, as outlined in Recital 43, and the obligation to document reasons for refusing to comply with a data subject access request under Article 15(4), further enhancing controller accountability.[316] Finally, where information on restriction grounds can also not be provided, data subjects retain the possibility to lodge a complaint with the supervisory authority or seek effective remedy.[317] **Given the margin of discretion afforded to Member States, the value of these rights will be further assessed in practice** (see below under national implementations).

[310] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017. See also Leiser, M. and Custers, B., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78.

[311] Se by contrast Article 21 of GDPR.

[312] Articles 13(2) and 16(4) of LED.

[313] Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' Privacy Technologies and Policy, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30; Vogiatzoglou, P., Quezada Tavárez, K., Fantin, S. and Dewitte, P., 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 11, No 3, 2020, pp. 274–302.

[314] Article 15(2) of LED.

[315] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873; Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' *Privacy Technologies and Policy*, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30.

[316] Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' *Privacy Technologies and Policy*, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30.

[317] Article 15(3) of LED.

4.3 Further derogations

Article 17 governing the exercise of data subject's rights by the supervisory authority is foreseen as a safety net for both competent authorities and data subjects.[318] Competent authorities may decide not to disclose any verification of processing whatsoever in order to safeguard ongoing investigations[319], while data subjects are given the opportunity to have at least the lawfulness of their data processing verified by the supervisory authority[320]. According to WP29, the so called right of 'indirect' access as laid down in Article 17 is to be distinguished from the right to lodge a complaint with the supervisory authority under Article 52, and constitutes an additional right in the framework of the LED.[321] WP29 has further argued that, **despite the ambiguous LED wording, supervisory authorities should be given the power by national law to exercise not only the right of access but the rest rights of rectification, erasure and restriction on behalf of the data subjects.**[322] The same understanding is adopted within literature, which perceives this power by supervisory authorities as a sort of independent oversight of the lawfulness of processing, in line with the abovementioned ECtHR jurisprudence[323].[324]

Supervisory authorities should treat requests and replies pursuant to Article 17 with outmost diligence, upholding this delicate balance between the interests of data subjects and competent authorities.[325] **In practical terms, however, this balance may prove rather challenging to achieve;** the supervisory authority may not always be in a position to detect irregularities or ensure the rectification of data, while their response may have to be approved by the competent authority denying direct access.[326] The question then arises how a data subject can pursue their case in court if they do not have access to their data and might not know whether the supervisory authority remedied any irregularity.[327]

A significant limitation of the LED data subject's rights is stipulated under Article 18, which allows Member States to designate national law as the applicable framework for the exercise of rights 'where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings'. The possibility to derogate from the data subject's rights as laid down in the LED by virtue of national criminal procedural laws is further reiterated in Recitals 49 and 107. It is unclear whether record and case file are to be understood as judicial record and judicial

[318] See also Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', *Global Privacy Law Review*, Vol. 1, No. 2, 2020, pp. 93–103.

[319] Articles 13(3), 15(3) and 16(4) of LED.

[320] Article 17(3) of LED.

[321] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 23-24.

[322] Ibid.

[323] *Roman Zakharov v. Russia,* App. no. 47143/06, 11 December 2015, paragraphs 272-285; *Szabó and Vissy v.* Hungary, App. no. 37138/14, 12 January 2016, paragraphs 75-77

[324] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

[325] Ibid.

[326] Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' *Privacy Technologies and Policy*, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30.

[327] Ibid.

case file, as well as in which instances this derogation may apply, given that different national criminal procedural laws make it difficult to determine what phase of a prosecution is referred to.[328]

The purpose of Article 18 was questioned during the fifth CEG meeting; in the Commission's view, it is meant to ensure that the same guarantees can be provided elsewhere, while another Member State argued that most of the rights already exist in the criminal procedural law.[329] However, along with Recital 20 mentioned above under section 2 in relation to the scope of the LED, and Article 45(2) on limiting supervisory authorities competences, as discussed below, this provision is claimed to create the risk of a 'black hole' allowing Member States not to apply data protection rights and obligations.[330] **The real added value of the LED rights therefore depends on the Member State's willingness, as well as potential future interpretations by the CJEU.**[331] **A detailed overview of the transposition of Chapter III within Member States, including federal regimes and national criminal procedural law provisions, should be provided.**[332]

4.4 National implementations

National transposing laws

An empirical study conducted in 2020, in which one of the authors of this report participated, has documented the diverse national implementations of Articles 12-15, as well as the processes of exercising the right of access in practice within Belgium, Cyprus, France, Greece, Ireland, Italy, Luxembourg, Malta, the Netherlands and Portugal.[333] While a detailed analysis of the national frameworks and practices may be found in the respective publication[334], a summary is presented as follows:

On Article 12: insofar as timing, fees and denials of requests are concerned, only the Portuguese law[335] requires competent authorities to respond within a specific timeframe (thirty days, renewable for

[328] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70.

[329] Commission Expert Group, Minutes of the fifth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 18 January 2017.

[330] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70.

[331] Di Francesco Maesa, C., 'Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)', *Eurojus Italia*, 24 May 2016, http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/.

[332] Chairman of Committee on Civil Liberties, Justice and Home Affairs, 'LIBE Contribution to the Commission upcoming report on the evaluation and review of the Law Enforcement Directive', IPOL-COM-LIBE D (2022)3535, 7 February 2022.

[333] Vogiatzoglou, P., Quezada Tavárez, K., Fantin, S. and Dewitte, P., 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives', *Journal of Intellectual Property, Information Technology and E-Commerce Law,* Vol. 11, No 3, 2020, pp. 274–302. While the UK was also included in the study and the paper, it is not mentioned herein.

[334] Ibid.

[335] Article 13 of Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Diaro da Republica 151 p. 41, 8 August 2019).

another thirty). Italy[336], Belgium[337] and the Netherlands[338] stipulate that the provision of information must respect domestic limitations arising from police statutes and criminal procedures. Greece[339], Ireland[340] and Italy[341] expect that the contact details of the controller should be found online on the controllers' website.

On Article 13: research suggests that national formulations differ from the LED for numerous Member States. For example, in Portugal[342], the controller must make information 'publicly available and permanently accessible' regardless of a data subject request, and the Belgian law[343] does not distinguish between Articles 13(1) and 13(2), thereby suggesting that the controller shall in any case provide all information listed therein.

On Article 14: only a few national laws have adopted a different wording or additional requirements. In the Dutch law[344] a specific timeframe for a response from the controller is set, while France[345] lays down a specific procedure for the identification of the data subject, who must prove their identity by any means (including using digital identity) that is deemed sufficient by the controller for the authentication. During said identification process, the response period is suspended.

On Article 15: noteworthy differences were identified within some national laws. For example, the Portuguese transposition[346] does not seem to require controllers to document the factual reasons for

[336] Article 9 of Attuazione della direttiva UE 2016/680 del Parlamento Europeo e del Consiglio, del 27.4.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Gazzetta Ufficiale della Repubblica Italiana 119, 24 May 2018).

[337] Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018).

[338] Articles 24a and 26(1) of Wet van 21 juli 2007 houdende regels inzake de verwerking van politiegegevens (Wet Politiegegevens, Stb. 2007, 549).

[339] Article 57 of Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις (Εφημερίς της Κυβερνήσεως Α137 p. 03379; 29 August 2019).

[340] Section 90 of Data Protection Act 2018 (Act 7 of 2018) (Iris Oifigiúl 42 p. 00752, 24 May 2018).

[341] Article 10 of Attuazione della direttiva UE 2016/680 del Parlamento Europeo e del Consiglio, del 27.4.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Gazzetta Ufficiale della Repubblica Italiana 119, 24 May 2018).

[342] Article 14 of Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Diaro da Republica 151 p. 41, 8 August 2019).

[343] Article 37 of Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018).

[344] Article 25 of Wet van 21 juli 2007 houdende regels inzake de verwerking van politiegegevens (Wet Politiegegevens, Stb. 2007, 549).

[345] Article 135 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés as amended by Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (Journal Officiel de la République Française, 3 August 2018).

[346] Article 16 of Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a

refusing to respond to a data subject access request. By contrast, in Cyprus[347], the denial from the controller must be validated after consultation with the national supervisory authority, which is the one responsible for adopting a list of processing categories that may be subject partly or wholly to restriction.

The Opinion by the Lithuanian supervisory authority on the draft law transposing the LED raised several concerns regarding Chapter III of the LED, which seem to remain valid in the final text of the adopted law[348].[349] More specifically, the transposition of Article 13(2), (3) and (4), instead of defining in itself pursuant to the LED wording, allows the controller to determine the 'specific cases', the delay, restrictions or omission of provision of information as well as the categories of processing that may wholly or partly be subject to restriction. Additionally, Article 15(2) regarding the documentation of refusal is not properly specified.

In Denmark, competent authorities do not have to motivate refusals of access.[350] The Czech transposition allows controllers not to comply with the right of access when doing so would endanger the performance of a task within the context of the LED.[351] The controllers must in that case keep a record of the reasons justifying the refusal for a period of three years.[352]

Pursuant to the German transposition[353], the controller may postpone, restrict or omit the information requirements of Article 13, upon the listed conditions reflecting Article 13(3), and upon an assessment that the prevention of danger outweighs the interest in informing the data subject. The additional balancing test between interests indicates a further safeguard against abuse of restricting information rights.[354] Moreover, the German law[355] requires that when the recipients of data are national security authorities such as intelligence services, then information about these recipients could be given to the data subject only if the concerned recipient gives their agreement. In this case, the recipient enjoys a wide margin of appreciation which lies beyond the control of the data controller. Additionally, the German legislator has added new grounds of access refusal[356]; the controller may restrict the right of access also when data are stored only due to legal requirements or they are used only for purposes of

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Diaro da Republica 151 p. 41, 8 August 2019).

[347] Article 17 of Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα από Αρμόδιες Αρχές για τους Σκοπούς της Πρόληψης, Διερεύνησης, Ανίχνευσης η Δίωξης Ποινικών Αδικημάτων ή της Εκτέλεσης Ποινικών Κυρώσεων και για την Ελεύθερη Κυκλοφορία των Δεδομένων Αυτών Νόμος του 2019 (Cyprus Gazette 4694 p. 267, 27 March 2019).

[348] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale (Journal officiel du Grand-Duché de Luxembourg A 689 p. 1, 16 August 2018).

[349] Commission nationale pour la protection des données (Luxembourgish supervisory authority), 'Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7168 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification de certaines lois, Délibération n° 1049/2017 du 28 décembre 2017.

[350] Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020, p. 77.

[351] Section 28 of Zákon ze dne 12. března 2019 o zpracování osobních údajů (Aktuální znění 24.04.2019).

[352] Ibid.

[353] §56 of Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).

[354] Hudobnik, M., 'Data Protection and the Law Enforcement Directive: A Procrustean Bed across Europe?', *ERA Forum*, Vol. 21, No. 3, 2020, pp. 485–500.

[355] §57 of Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).

[356] Ibid.

data security or data protection audits, when granting the right of access would pose disproportionate effort and all measures have been taken to prevent their processing for other purposes. The right of access could be denied also if the data subject does not provide sufficient information allowing the controller to locate their personal data without disproportionate effort. It is questionable whether these grounds are in line with the LED.[357] In fact, a request for preliminary ruling has been lodged before the CJEU on the interpretation of Article 15 LED, the compatibility of the German transposing law and the relation between Article 15 LED and Article 47 Charter on the right to an effective remedy.[358]

The most striking transposition of Chapter III of the LED is the one by the Belgian legislator[359], offering data subjects only the possibility of an indirect exercise of their rights, through the national supervisory authority, obviously against the wording of the LED.[360] Moreover, the Belgian supervisory authority[361] may only conduct the necessary verifications, which is the minimum foreseen under Article 17(3). The requirement upon the supervisory authority to inform the data subject of their right to seek a judicial remedy under Article 17(3) LED has not been transposed into Belgian law. A request for preliminary ruling regarding Article 17 LED and the compatibility of this practice by the Belgian supervisory authority with Articles 47 and 8(3) Charter has been lodged before the CJEU.[362]

Concerns about an incorrect implementation of Article 17 have also been raised by the Greek supervisory authority, which pointed out how the Greek law transposed Article 17 merely as a possibility to raise a complaint through the supervisory authority instead of providing for an indirect exercise of data subject's rights.[363] Finally, the Irish transposition of Article 17 includes a clause ensuring that '[n]othing in this section shall require the Commission to disclose to a data subject whether or not a controller has processed, or is processing, personal data relating to him or her'[364], demonstrating a level of tension between access rights and public interest.[365]

With respect to Article 18, it has been reported that the majority of Member States foresee that data subject's rights can be exercised in accordance with national law in the context of national criminal investigations and proceedings, although the conditions thereof are not always clear.[366] This is the case, for example, in Lithuania, whereby the Lithuanian supervisory authority expressed their doubts whether the national safeguards are higher than the ones provided in the LED.[367]

---

[357] Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' *Privacy Technologies and Policy*, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30.

[358] Request for a preliminary ruling, *TX v Bundesrepublik Deutschland*, C-481/214, August 2021.

[359] Article 42 of Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018).

[360] Vogiatzoglou, P., Quezada Tavárez, K., Fantin, S. and Dewitte, P., 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives', *Journal of Intellectual Property, Information Technology and E-Commerce Law,* Vol. 11, No 3, 2020, pp. 274–302.

[361] Organe de contrôle de l'information policière – Controleorgaan op de Politionele Informatie.

[362] Request for preliminary ruling, *Ligue des droits humains*, C-333/22, 20 May 2022.

[363] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Greek supervisory authority), Γνωμοδότηση 1/2020, Athens 24 January 2020.

[364] Section 95(4) of Data Protection Act 2018 (Act 7 of 2018) (Iris Oifigiúl 42 p. 00752, 24 May 2018).

[365] Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020, p. 36.

[366] Moscibroda, A., 'Law Enforcement Directive 2016/680: General principles and transposition', *Data Protection and the Law Enforcement Directive*, ERA Online Seminar, June 2020.

[367] Commission nationale pour la protection des données (Luxembourgish supervisory authority), 'Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7168 relatif à la protection des personnes physiques à

The European Commission report notes that all national laws restrict the right of access under Article 15 LED, while most also foresee restrictions for other data subject's rights pursuant to Articles 13(3) and 16(4) LED.[368] Moreover, most national laws have transposed Articles 17 and 18 LED. However, several national laws do not fully specify the requirements for the exercise and the restriction of rights.[369]

Exercise of data subject's rights

The 2020 empirical study further documented the researchers' experience with the process of looking for information on data processing online and submitting data subject access requests before competent authorities in Belgium, Cyprus, France, Greece, Ireland, Italy, Luxembourg, Malta, the Netherlands and Portugal.[370] While a detailed analysis of the experience documented by the researchers may be found in the respective publication[371], most notable practices are briefly presented herein. In their (subjective) opinion, finding information about processing by competent authorities online varied amongst Member States, with some websites providing very easily accessible information (like Cyprus or Luxembourg National Police) and others offering a more complex presentation (like Belgium's or the Netherland's authorities). Information related to data protection policies was included under a dedicated section on most websites, with few gathering different links for each policy of different police databases (like Italy). Except for Portugal, all competent authorities included the information requested by Article 13(1) within their dedicated webpages. Furthermore, some websites provided additional information such as general retention policy (Italian Police), basic data protection principles (Irish Police) or security of processing (Luxembourg Police). With the exception of the Portuguese Police, all competent authorities' websites also included instructions on how to file an access request. Only Ireland, Italy and the Netherlands provided a template to be filled in by data subjects, while the French template was found in the website of the French supervisory authority.

When it came to the submission by the researchers of data access requests, most competent authorities accepted submissions in an electronic format, while France, Italy and the Netherlands required them to be sent via regular post. Surprisingly, even though requests had been sent via post, the French Ministry of Home Affairs responded via email, declaring the requests as inadmissible with the reason that 'such a request is only admissible if sent via postal mail', and also as manifestly abusive for being too broad (see also below). As additional requirement, the Luxembourgish authorities required an official address certificate. The Irish police asked for a proof of residence and a list of all previous addresses in the country, requirements that not only were not expressly stipulated in the Irish transposing law, but also seem to go against the LED which does not foresee any such restriction of the LED right to nationals of a Member State only. By contrast, Recital 17 explicitly foresees the applicability of the LED afforded protection to natural persons regardless of their nationality of place of residence. Following up on the requests, reminders had to be sent only to the Cypriot, Greek and Maltese authorities.

---

l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification de certaines lois, Délibération n° 1049/2017 du 28 décembre 2017.

368 European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 15.

369 Ibid.

370 Vogiatzoglou, P., Quezada Tavárez, K., Fantin, S. and Dewitte, P., 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives', *Journal of Intellectual Property, Information Technology and E-Commerce Law,* Vol. 11, No 3, 2020, pp. 274–302.

371 Ibid.

Overall, most requests were fully processed and resulted in responses by the corresponding authorities, either indicating that no data about the data subjects (the researchers in question) were being processed, or simply confirming that personal data about them were being processed. In addition, the Greek competent authority provided a list of all the categories of data they held as well as the legal basis for processing (though not the personal data as such), while the Dutch response contained a detailed list of databases consulted. However, none of the responses disclosed all the pieces of information listed in the LED. The French competent authority refused to comply on the grounds that the requests were 'manifestly abusive' given their overly broad scope, while the Portuguese competent authority refused on the basis of lack of compliance with all the formal requirements; yet, the alleged lack of compliance related to requirements that were not specified in Portuguese transposing law. Whereas the Belgian and Maltese competent authorities were the fastest to provide the final responses, the Irish, French and Italian were amongst the last, and the Luxembourgish was the last to respond, over six months after the initial requests.

A number of conclusions can be drawn with regards to the 10 Member States investigated in the 2020 empirical study: the diverse implementation of information obligations and data subject's rights amongst the Member States in question seem to lean more towards expanding the discretion of competent authorities. Moreover, exercising data subject's rights in practice remains complicated and challenging within the EU, and Member States should put more effort in the presentation of clear, coherent and transparent information on data processing, for example by providing for single points of information. The process of submitting rights' requests could be streamlined, for instance through the creation of templates as well as types of responses on an EU level. Seemingly arbitrary procedural requirements, such as list of addresses within the country, should be reconsidered. In that regard, it should be questioned whether data subject's rights should be limited to residents of each Member State, or established on a broader European level. **Further guidance on the modalities for providing information and responding to data subject's rights requests by national supervisory authorities and European data protection bodies is encouraged.**[372]

Nevertheless, it should be noted that more recent documents, including the Council position and findings on the application of the LED from November 2021[373], the EDPB contribution to the European Commission's evaluation of the LED from December 2021[374], and the European Commission report that builds on the previous documents[375], **demonstrate a heightened awareness on data protection within criminal justice.** More specifically, the Council notes an increase in the number of data subject's requests before competent authorities, demonstrating an increased awareness amongst data subjects of their rights, which further contributed to an elevation of competent authorities' data protection

[372] See also ibid.

[373] Council position and findings on the application of the 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, 13943/21, 18 November 2021.

[374] European Data Protection Board, Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, 14 December 2021.

[375] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 16-18.

awareness as well.[376] Practical experience reported to the Council shows that data subjects are primarily exercising their rights of access and erasure.[377]

When it comes to feedback from supervisory authorities on data subject's rights, more than a third of them report an increase in the number of complaints received[378], which is logical given that rights and obligations for domestic processing activities by criminal justice actors have only been established by the LED. The supervisory authorities further report a diversity of issues raised in the complaints, mostly relating to the right of access and limitations thereof (Articles 14-15 LED), and the right to rectification or erasure (Article 16 LED).[379] Fewer complaints related to the right to information (Article 13 LED) and the modalities for exercising the rights of data subjects (Article 12 LED).[380]

Moreover, it seems that most supervisory authorities keep statistics on the indirect exercise (Article 17 LED). Approximately half of them received such requests, with France having received the most (1553) and Croatia the least (1).[381] The outcomes of the requests were diverse; in most cases the supervisory authority confirmed that the necessary verifications had taken place and/or that the request was inadmissible.[382] In several cases, the requests resulted in the obligation upon the controller to rectify or erase personal data or restrict processing, in some cases, access to personal data was provided, while one supervisory authority reported to have applied its corrective powers as a result of such request.[383] Most supervisory authorities did not report particular problems with the indirect exercise of data subject's rights under Article 17 LED, as transposed into national law.[384]

[376] Council position and findings on the application of the 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, 13943/21, 18 November 2021.

[377] Ibid.

[378] European Data Protection Board, Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, 14 December 2021, p. 10.

[379] Ibid.

[380] Ibid.

[381] Ibid, p. 15.

[382] Ibid.

[383] Ibid.

[384] Ibid.

5. CONTROLLER OBLIGATIONS

KEY FINDINGS

Concerns have been raised regarding the opacity and lack of accessible information regarding joint controllership in Article 21 LED. This risks complicating the exercise of data subject rights and is compounded further by the inconsistent national implementation of the establishment of a single point of contact.

The implementation of logging mechanisms pursuant to Article 25 LED stands to improve the accountability of data controllers and should receive regular and continuous attention. As anticipated in Article 62 LED, the deployment of these measures appears difficult and slow-going. Additionally, certain aspects of the logging requirement are prone to misinterpretation and national details on the use and management of logs appear limited despite previous recommendations. While system logs are to be used proactively, caution is due to avoid that they are processed for unrelated purposes.

Regarding the Data Protection Impact Assessment, the comparatively limited detail provided in Article 27 LED remains a serious cause for concern. This is exacerbated by the various unclarified concepts and a significant lack of concrete guidance on DPIAs in the context of law enforcement and criminal justice, as materials applicable to the GDPR are not equivalently applicable in this sphere. Leaving the interpretation and application of this process to the discretion of national competent authorities and supervisory bodies risks undermining its utility.

The LED contains robust requirements for data security. While it might be preferable for all Member States to have implemented the extensive list of controls provided for by Article 29 LED, high standards for data security appear to be present in national law. Nevertheless, discrepancies exist with regards to the application of these provisions at the national level and further harmonization of data breach procedures is recommended.

5.1 Joint controllers

In order to effectively investigate, prevent and prosecute criminal activity, public authorities in the sphere of law enforcement and criminal justice are often required to cooperate with various entities. Such instances of collaboration can occur both between separate departments within the same organization as well as with involve external actors, agencies or institutions.. While these coordinated operations and instances of collaboration between different agencies and institutions are an effective method of policing and often vital in the fight against crime, they nevertheless raise concerns regarding accountability and demonstrating compliance with data protection norms. To this end, Article 21 LED establishes a number of rules for the event that two or more controllers jointly determine the purposes and means of the processing operations. In such a situation, they are to determine their respective responsibilities for legal compliance by means of an arrangement, unless these responsibilities are instead established by a legal act, and must designate a single point of contact for data subjects. Drawing upon a comparison with its counterpart in Article 26 GDPR, legal scholarship has raised a number of remarks that deserve mention.[385]

[385] Radtke, T., 'The Concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in Contrast to the GDPR', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law,* Vol. 11, No. 3, 2020, pp. 242-251.

First, Article 21 LED reiterates the requirement of the GDPR that the determination of the joint controllers' respective responsibilities must occur in a 'transparent manner'. This is a notable inclusion since, as mentioned in section 3 and contrary to the GDPR, the LED does not cite transparency as a general principle of data protection.[386] While the CEG has suggested that 'some degree of transparency' is implied by the principle of fairness[387], it remains unclear to which extent this is the case as the sensitive nature of law enforcement processing inherently begets a greater degree of confidentiality. This might thus suggest that the obligation of transparency regarding joint controllership is subject to greater restrictions under the LED, although the lack of further clarification leaves it up to the Member States to determine how transparent this collaboration must be. Similarly, the LED does not instate an obligation to inform data subjects of the essence of the arrangement and, consequently, the nature of their relationship and cooperation. While the direct impact of this is likely to be limited, it risks complicating the exercise of data subject rights.

Accordingly, it has previously been recommended that national legislators take further steps to incorporate the requirements under Article 21 LED into the broader obligations of providing information that data controllers must adhere to under Article 13.[388] As discussed in section 3, the controller is to make certain information available to the data subject pursuant to this provision, although no stipulations are included regarding the point of contact or the abovementioned transparency requirement regarding the respective responsibilities of joint controllers in view of the exercise of data subject rights. **At present, it appears the inclusion of details regarding joint controllership under the general requirements of providing information to data subjects is not commonplace among Member States.** As further discussed below, there appears to exist a significant degree of deviation among Member States regarding the approach to joint controllership, and none of the examples of national legislation discussed hereafter seem to have incorporated further details regarding joint controllers into their general provisions on the provision of general information to data subjects.

Second, the LED diverges from the GDPR concerning the contents of the arrangement in question. Under the GDPR, this arrangement is to 'duly reflect the respective roles and relationships' in view of the data subjects and make available the 'essence' of their agreement. The absence of such a clause in Article 21 LED has been criticised by legal scholars as its inclusion could have encouraged the controllers to exercise more self-control and have a heightened awareness of their respective obligations under data protection law.[389]

Third, a noteworthy balancing exercise can be observed regarding the inclusion of certain requirements.[390] On the one hand, the GDPR mandates that data subjects have the opportunity to exercise their rights against each of the controllers, meaning that they face joint and several liability for the violation of data protection norms. In the LED, however, it remains up to the Member States whether they want to adopt the same structure of liability for competent authorities. On the other hand, the LED necessitates that joint controllers identify a single point of contact for data subjects,

---

386 De Hert, P. and Sajfert, J., 'The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680', Brussels Privacy Hub Working Paper 7, no. 31, December 2021.

387 Commission Expert Group, Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 November 2016.

388 Radtke, T., 'The Concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in Contrast to the GDPR', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 11, No. 3, 2020, 248.

389 Ibid., 245.

390 Ibid., 247-248.

while the GDPR leaves it up to the controllers themselves to decide whether such a contact point is appropriate. As such, it appears that these instruments have taken a slightly different approach to the measures deemed most suitable for the exercise of data subject rights, with the LED's mandatory contact point contributing 'almost as effectively' to their protection as the GDPR according to some experts.[391]

Lastly, **a critical remark is in order with regard to the apparently inconsistent national implementation of Article 21 LED**.[392] In particular, there appear to exist discrepancies regarding the incorporation of the provision's general requirements and the establishment of the contact point. For instance, the Dutch Act on Police Information contains no separate provision regarding joint controllership. Instead, it stipulates that there will only ever be a single controller in the context of the LED, as the controller tasked with the actual management of the data processing and implementation of measures relating to data accuracy, security and data protection by design will in practice be viewed as the sole controller.[393] Nevertheless, Article 31d of this Act still mandates that data controllers keep records of the identity and contact details of 'joint controllers', thus leaving in place an apparent discrepancy in national law. Furthermore, the German Data Protection Act makes no explicit mention of the obligation to designate a contact point for joint controllership, thereby seemingly leaving this requirement of the LED absent from its national legal framework altogether.[394] And while both the Irish and Belgian data protection laws do make mention of this contact point, they leave it up to the discretion of the controllers whether they will provide in a single point of contact.[395] This could thus be indicative of some interpretative confusion as Article 21 LED prescribes that the arrangement must designate a contact point for data subjects but that it remains up to the Member States to designate which of the controllers shall act as the single point of contact. As such, it appears that this stipulation is intended to signal that there must always be a singular point of contact, but that it is up to the discretion of the Member States to determine which controller takes on this role. Instead, certain countries seem to have interpreted this as meaning that they are to decide whether such a contact point is even needed at all. **Further clarity and consistency on this matter would thus be welcomed.**[396]

5.2 Logging and recordkeeping

As a key objective of the LED is to foster a high level of accountability for the processing of personal data, it is vital that competent authorities are able to demonstrate compliance with the Directive and that supervisory bodies have the ability to review the lawfulness of their processing activities. To this end, Chapter IV of the LED introduces the requirements of logging and recordkeeping. Pursuant to Article 24, controllers and, to a lesser extent, processors must maintain a record of all categories of processing operations under their responsibility. Among others, these records must contain

391 Ibid., 247.

392 Ibid., 248.

393 See Art. 1.f.4° Wet van 21 juli 2007 houdende regels inzake de verwerking van politiegegevens (Wet Politiegegevens, Stb. 2007, 549) and the Dutch Raad van State Explanatory Memorandum on the Implementation of the LED, p. 84, https://www.raadvanstate.nl/publish/pages/108235/w-16-17-0366.pdf

394 Art. 63 Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).

395 Art. 52 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 September 2018) and Art. 79 Data Protection Act 2018 (Act 7 of 2018) (Iris Oifigiúl 42 p. 00752, 24 May 2018).

396 In this context, reference must be made to a recent request for a preliminary ruling to the CJEU in which the question is raised whether the identity of the entities actually involved in instances of joint data processing ought to be named and whether access thereto can be denied without the provision of substantive reasons. For more, see: Request for a preliminary ruling, *TX v Bundesrepublik Deutschland*, C-481/214, August 2021.

information on the purposes of the processing, the relevant legal basis, the retention and security of data, the disclosure to other recipients, and the categories of data subject and personal data involved. This provision thus requires that the competent authorities document their activities and are able to disclose this information to the supervisory authorities upon request.

By contrast, the requirement of logging imposes a more extensive obligation for competent authorities to track and record certain activities. Under Article 25, Member States must provide for logs to be kept for various processing operations in automated processing systems, including at least the collection, alteration, consultation, disclosure, combination and erasure of personal data in computer systems. Of particular importance are the logs of consultation and disclosure, as they must allow for the establishment of the justification, date and time of the processing, and, where possible, the identification of the individuals who consulted, disclosed or received the data. This information must be made available to the competent authorities on request and are only to be used for the verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings. Accordingly, these logs do not concern general information regarding the processing activities, as is the case with the abovementioned records, nor do they require that the content of the data itself is registered. Instead, they require competent authorities to produce and preserve metadata in their IT systems that contains specific information on how and by whom certain personal data was managed.[397]

As a result of the above, the requirement of logging has received notable scholarly attention. **Seen as a significant improvement to the accountability of law enforcement data processing, the logs are deemed to play a central role in addressing data misuse and restricting access to individuals with the proper credentials and valid motivations to process the data at hand.**[398] In particular, the inclusion of the justification requirement for the consultation and disclosure of data stands out as an innovative and potent step towards accountability. Given that the exact content and functioning of the logs is dependent on the national configurations of the systems in use, the LED does not provide additional details on their practical application but instead remains technology-neutral and leaves their further specification to the Member States.[399]

At the national level, it appears that most Member States have transposed Article 25 in a consistent manner.[400] While some discrepancies exist regarding the specific conditions, national data protection legislation generally employs a similar approach to the logging of law enforcement data processing and meets the general objectives of this provision.[401] In practice, the inconsistencies that do exist are often grounded in Member States going beyond what the LED requires. As Article 25 merely establishes a minimal set of operations that must be subject to logging, various European countries have further expanded upon this condition by instituting additional safeguards. Austria, for example, establishes stricter and more extensive rules on the keeping of logs by applying these conditions to all processing

---

397 Information Commissioner's Office (ICO), 'Guide to Law Enforcement Processing – Logging', 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

398 Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

399 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, 26.

400 Moscibroda, A., 'Law Enforcement Directive 2016/680: General principles and transposition', *Data Protection and the Law Enforcement Directive*, ERA Online Seminar, June 2020.

401 Hudobnik, M., 'Data Protection and the Law Enforcement Directive: A Procrustean Bed across Europe?', ERA Forum, Vol. 21, No. 3, 2020, pp. 485–500.

operations and explicitly mandating that they must allow for the tracing and checking of the processing's admissibility.[402]

Despite this apparent high level of national consistency, note must be made of a particular aspect of this provision. **Since the producing of logs in computer systems is an inherently technical task, concerns can be raised regarding its practical implementation.** As it stands to reason that not all programs used by law enforcement provide in the functionality to record metadata, identify individual persons or allow users to submit a justification for their use of the system, it could prove technically and financially challenging to update and alter these tools to include such features.[403] To pre-emptively account for this complication, Article 62(2) and (3) LED allow Member States to derogate from the Directive's default two-year transposition period and exceptionally delay the implementation of Article 25(1) until May 2023, when bringing the automated processing systems in conformity would involve disproportionate effort, or until May 2026, if doing so would cause serious difficulties for the operation of the system and the Commission is notified of these grounds.

In practice, it seems that these concerns were well-founded as adapting all relevant systems by May 2018 would likely have been an impossible feat. As illustrated by surveys of law enforcement representatives, not all police systems are currently equipped with the capabilities of producing the required logs.[404] In Denmark, for instance, respondents noted that the logging of processing operations is not to commence until 2023 despite the fact that this does leave a security risk due to the possibility of abuse. In Ireland, the Data Protection Act includes an explicit acknowledgement of this derogation by exempting controllers and processors from maintaining the required logs until 2023 or 2026 if doing so would, respectively, involve disproportionate effort or cause serious difficulties for the operation of the system.[405] In case of the latter, the Act even establishes a procedure by which competent authorities are required to notify the Minister of their intention to postpone compliance. And in the Netherlands, the provision regarding logging has yet to be further specified and enter into force, thus leaving a currently blank article in place.[406] Given the difficulty associated with the implementation of the logging requirements, regular attention should be paid to the national standing of police systems being brought in conformity with Article 25 LED.

Furthermore, three additional facets of the logging requirements deserve additional remarks. First, it is highly recommended that the logs are evaluated in a proactive manner that involves both internal and external monitoring, as data protection experts have previously highlighted the key role of supervisory authorities and encouraged their active involvement in reviewing the logs.[407] While Article 25 LED merely asserts that the logs must be provided to the supervisory authorities upon their request, it is advisable that they actively and regularly review them to monitor compliance with data protection law and to ensure that violations of the data management policies are properly addressed. Similarly, it has been suggested that the data controllers themselves engage in frequent self-auditing and periodical

---

402 Article 50 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG, 25 May 2018).

403 Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

404 Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020, p. 79.

405 Article 82 Data Protection Act 2018 (Act 7 of 2018) (Iris Oifigiúl 42 p. 00752, 24 May 2018).

406 Article 32a Wet van 21 juli 2007 houdende regels inzake de verwerking van politiegegevens (Wet Politiegegevens, Stb. 2007, 549).

407 Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

analysis of the logs, potentially by automated means.[408] **It is thus recommendable that the data processing logs are not just examined in the event of a data breach or abuse of power but instead used proactively and on a continuous basis.**

Second, it is important that Member States employ a consistent interpretation of the use of logs 'for criminal proceedings'. In line with the policy motivations behind the provision, the logging requirement is intended to facilitate a greater degree of police accountability. As asserted by WP29, a narrow interpretation of this stipulation is in order and the use of logs during criminal proceedings must be limited to those related to data breaches, the security or integrity of the data, or the potential unlawfulness of police processing operations.[409] This, however, might not be clear in all national data protection legislation. In Belgium, for example, the corresponding provision of its data protection act merely states the logs may only be used for the general purposes of the LED as noted by Article 1(1) of the Directive.[410] As such, it is not unthinkable that this provision might be interpreted in an overly broad fashion leading to the unintended use of the logs for various police operations and as evidence in general criminal proceedings rather than just those involving system use and data access. **Accordingly, caution is due in order to avoid that Member States make use of these logs in unrelated proceedings, investigations or prosecutions.**

Lastly, further attention may be warranted for certain remarks made by WP29. In its opinion, the Working Party strongly urged the adoption of national laws that further develop various aspects of the logging requirements, including the technical measures taken to implement them, the storage periods of the logs, their exact content, and the internal policies on self-auditing and legal compliance.[411] At present, national adherence to these recommendations seems limited albeit not quite non-existent as certain Member States have incorporated further details and more extensive rules in their legislation. For instance, the German Data Protection Act determines periods for the storage of the logs by requiring that they are deleted before the end of the year following their production[412]. Similarly, the Netherlands mandates that data controllers conduct periodic privacy audits and disclose the results to the supervisory authority, yet it remains unclear what these audits will entail and how they might function in absence of a provision on logging.[413] Regardless, such stipulations do not appear to reflect widespread practice in national law. While it remains possible that similar procedures have been incorporated in internal policy documents instead, it seems that limited action has been taken to incorporate the Working Party's recommendations during the transposition of Article 25 LED. **Upon further review, it might be advisable that a renewed focus is placed on expanding the national rules on logging in conjunction with Member States aligning their systems with these requirements before 2023.**

---

[408] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, 26.

[409] Ibid., 27.

[410] Article 56§1 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018).

[411] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, 28.

[412] Article 76(5) German Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).

[413] Article 33 Wet van 21 juli 2007 houdende regels inzake de verwerking van politiegegevens (Wet Politiegegevens, Stb. 2007, 549).

5.3 Data Protection Impact Assessment

In order to better demonstrate compliance with legal norms and negate adverse effects before they arise, the EU data protection reforms require that a DPIA is conducted before high-risk processing activities are allowed to take place. Present in both the GDPR and LED, this requirement entails that data controllers both assess the potential impact of the envisioned operations on the rights and freedoms of individuals, and take appropriate steps to address the risks at hand and safeguard the interests of the relevant data subjects. In the LED, Article 27 determines the scope, details and requirements of this procedure in the context of law enforcement and criminal justice. It stipulates that a DPIA is in order when a type of processing, in particular where it involves the use of new technologies, is likely to result in a high risk to the rights and freedoms of natural persons when taking into account the nature, scope, context and purposes of the processing. This assessment must take place prior to the processing and contain a description of the envisaged operations, an evaluation of the risks to the rights and freedoms of data subjects, and an overview of the intended measures, safeguards and mechanisms used to address these risks and ensure the protection of personal data. As such, the DPIA does not concern individual cases but is instead meant to evaluate procedures, systems and general processing operations.[414]

The execution of a DPIA can be a powerful tool to promote compliance with data protection norms and human rights standards.[415] Building upon the well-established lineage of various types of impact assessments, DPIAs serve an important role in managing risky behaviours from a legal and ethical perspective.[416] By mandating that this assessment takes place prior to the processing, it complements the general principle of privacy by design[417] and provides both data controllers and system developers with a clear avenue to incorporate safeguards in the early stages of the development and planning of future data processing operations.[418] According to various scholars, the DPIA thus plays a critical role in improving the accountability of data controllers and strengthening the implementation of data protection safeguards.[419] This sentiment is shared by both the EDPB and the European Commission, as both have recently noted that the these impact assessments have improved the level of security in law enforcement data processing.[420] Regardless, some critical remarks on various aspects of the relevant provisions of the LED are in order.

First, it must be mentioned that there exist notable differences between the GDPR and LED in how they cover their respective stipulations regarding the data protection impact assessments.[421] Among others,

---

414 Recital 58 LED.

415 Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', *Computer Law & Security Review*, vol. 33, no. 3, 2017, pp. 324–340.

416 Raab, C., 'Information privacy, impact assessment, and the place of ethics', *Computer Law & Security Review*, Vol. 37, 2020.

417 Recital 53 LED.

418 Naudts, L., 'The Data Protection Impact Assessment for Law Enforcement Agencies', presented at the 12th International Conference on Communications, Bucharest, Romania, 15 June 2018.

419 Demetzou, K., 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation', *Computer Law & Security Review*, Vol. 35, 2019.

420 European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 19; European Data Protection Board, Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, 14 December 2021, pp. 21-22.

421 In this context, brief mention ought to be made of a notable divergence between data protection law and the abovementioned proposal for an AI Act. Under the GDPR and LED, the responsibility of assessing and mitigating risk falls on the data controller itself, which typically acts as the end-user of novel technologies. By contrast, the proposed AI Act instead requires the providers of AI systems to assess the risks associated with their tools and bring them into compliance with the Act's requirements. Some commentators have described this disparity as a misalignment and have

Article 35 GDPR establishes a clear list of the most prominent circumstances in which a DPIA is necessary, mandates the involvement of the controller's data protection officer in the process, and directs the national supervisory authorities to publish a list of the kind of processing operations that require the execution of a DPIA. Additionally, it provides further details on what the assessment must contain and necessitates that it includes an evaluation of the necessity and proportionality of the processing, the legitimate interests pursued by the controller, and a description of the operations that is 'systematic' in nature. By contrast, Article 27 LED contains no such clauses but instead relegates a number of factors relevant for the determination of risks to Recital 51. While this is further supplemented by WP29 recommending the execution of a DPIA when the processing involves sensitive data or engages in automated decision-making and profiling[422], **the LED nevertheless lacks the level of detail provided by the GDPR.**

Second, even though this does necessarily serve to the detriment of the LED, it is regrettable that comparatively little attention has been paid to providing concrete guidance on the execution of these assessments. As conducting a sufficiently thorough DPIA can be a complex endeavour and the risks associated with law enforcement data processing can arguably be more severe than those typically envisaged by the GDPR[423], there is clear value in providing competent authorities with consistent and extensive guidance on how to balance competing interests, evaluate the potential impact on human rights, and take proactive measures as to negate disparate effects. To this end, various European bodies[424], national data protection authorities[425] and legal scholars[426] have provided further insight into how such an assessment might be conducted. However, **the currently available guidance focuses primarily and often exclusively on complying with the GDPR, thus placing limited emphasis on processing operations by police and criminal justice authorities and lacking a EU-wide standard for DPIAs in this context.[427] This discrepancy is cause for concern as it risks creating interpretative issues**. Given that the LED and GDPR concern processing operations that can be entirely different in nature and that these instruments do not necessarily safeguard the same set of human rights[428], it is evident that instructions issued in the context of the GDPR cannot simply be applied to law enforcement processing.

---

recommended that the AI Act is amended to impose a similar obligation on system end-users. For more, see: Ebers M. et al., 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)', J Vol. 4, No. 4, 2021, pp. 589–603.

422 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p.14.

423 Ibid.

424 Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', WP248, 2017, https://ec.europa.eu/newsroom/article29/items/611236; European Data Protection Supervisor, 'Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation', 2019, https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf

425 See, for example, France Commission Nationale de l'Informatique et des Libertés (CNIL), 'Privacy Impact Assessment 1 (Methodology), 2 (Templates) and 3 (Knowledge bases)', July 2015, https://www.cnil.fr/en/privacy-impact-assessment-pia

426 Bieker, F. et al., 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' in *Privacy Technologies and Policy*, Cham, 2016, pp. 21–37.

427 For a more extensive overview of the currently available guidelines in this context, see: Marquenie, T. and Quezada-Tavárez, K., 'Data Protection Impact Assessments in Law Enforcement: Identifying and Mitigating Risks in Algorithmic Policing' in Markarian, G., Nitsch, H., Karlovic, R. and Chandramouli, K. (eds), *Security technologies and social implications: An European Perspective*, Wiley-IEEE Press, 2022 (under review).

428 Drechsler L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', *Global Privacy Law Review*, Vol 1, No. 2, 2020, pp. 93–103.

In addition, such guidance could prove useful in clarifying certain concepts used in both Article 35 GDPR and Article 27 LED. The notion of high risk, for example, has been described as 'unclarified' by data protection experts who have advocated for further clarity and a more comprehensive approach towards explaining this concept.[429] Similarly, the accompanying recitals introduce the notions of likelihood and severity, which have long been incorporated in risk assessments of different kinds, but neglect to provide further details on their interpretation. In stating that risks should be evaluated by means of an 'objective assessment' and that the elements of severity and likelihood must be considered in relation to the nature, scope, context and purposes of the processing, Recital 52 LED does little to illuminate how competent authorities are to balance and assess these different facets. **Leaving the interpretation of these provisions to the very limited number of national data protection authorities that have attempted to clarify this process for law enforcement actors[430] thus appears unlikely to result in a high and consistent level of protection across the EU.**

Third, this lack of robust guidance further appears to persist in spite of the vital role that DPIAs can play in demonstrating legal compliance. This holds particularly true in light of the deployment of novel police technologies that risk stigmatising minority groups, exacerbating unfair and discriminatory practices, and underlying an ever greater extent of state surveillance. Consequently, these tools pose unique and pressing threats to various human liberties and fundamental freedoms, including the rights to privacy and data protection, fair trial, free speech and equal treatment.[431] To illustrate this tension, reference can be made to recent case law from the United Kingdom. In the Bridges v. South Wales Police case from 2020, the UK Court of Appeal determined that the manner in which public facial recognition tools were used by the South Wales Police violated human rights law.[432] As one of the primary motivations behind this ruling, the Court noted that the DPIA applicable to the deployment of this technology had been conducted in an insufficiently thorough manner. In particular, it concluded that the assessment failed to present a proper examination of the impact on the fundamental rights at hand, and that it did not provide adequate measures to address the risks in question.[433] The Bridges case now serves as a cautionary reminder of the importance of the DPIA.

Although the European Commission's recent report on the LED notes that numerous national supervisory authorities have been involved in raising awareness on issues relating to data protection law[434], and that the process of conducting a data protection impact assessment was cited as an example of a topic that might be covered in this context, the availability of such guidance appears to

---

[429] Demetzou, K., 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation', *Computer Law & Security Review*, Vol. 35, 2019.

[430] The UK ICO is one of the only supervisory bodies to have provided specific guidance for the LED. See, Information Commissioner's Office (ICO), 'Guide to Law Enforcement Processing – Data Protection Impact Assessment', 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

[431] For more on assessing the impact of novel police technologies on human rights, see: Castets-Renard, C., 'Human Rights and Algorithmic Impact Assessment for Predictive Policing' in Micklitz, H.W., Pollicino, O., Reichman, A., Simoncini, A., Sartor, G., De Gregorio, G. (eds), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, 2021; Marquenie, T., 'Legal and Ethical Challenges in Algorithmic Policing and Law Enforcement AI' in Bourguignon, M., Hick, T., Royer, S., Yperman, W. (eds), *Technology and Society: The Evolution of the Legal Landscape,* Gompel & Svacina, 2020.

[432] R (on the application of Bridges) v Chief Constable of South Wales', UK Court of Appeal, EWCA Civ 1058, 2020. Accessed: Aug. 11, 2020. [Online]. Available: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

[433] Purshouse, J. and Campbell, L., 'Automated facial recognition and policing: a Bridge too far?", *Journal of Legal Studies*, April 2021.

[434] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 19.

have remained limited thus far. This is cause for concern. In absence of a rigorous assessment that not only accounts for the possible risks to data protection and human rights but also presents adequate steps to mitigate their adverse impact as intended in the LED, law enforcement operations that use novel technologies or otherwise entail high risks to the interests and freedoms of the data subject might well be ruled unlawful and terminated by national courts or supervisory authorities.[435] In light of the above, it is strongly recommended that consistent, thorough and EU-wide guidance is provided for DPIAs in the context of law enforcement and criminal justice.

5.4 Security of personal data

Ensuring a high degree of data security has become a priority of contemporary data protection law. While data protection and data security have long been intertwined[436], the ever growing importance of data in the digital society has elevated the role of security and safety in data processing. As such, the 2016 data protection reforms incorporated the security of personal data into its most fundamental principles.[437] In the LED, Section 2 of Chapter IV expands upon this principle by imposing additional obligations on data controllers with regards to the security of processing and the management of personal data breaches. Under Article 29, data controllers are to implement appropriate measures to ensure a degree of security that is appropriate to the risk, when taking into account the state of the art, costs of implementation, and that nature, scope, context and purposes of the processing as well as the severity and likelihood of the risks at hand. Pursuant to Articles 30 and 31, the supervisory authority must be notified of personal data breaches without undue delay, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons, and must similarly communicate the event to the data subject unless certain conditions would preclude them from doing so or make these communications unnecessary. With regard to Article 29, two points of interest are to be discussed.

First, this provision is particularly noteworthy as it is one of the few instances in which the LED appears to establish markedly stronger safeguards than the GDPR. While Article 32 GDPR contains the same general obligation of implementing technical and organisational measures that ensure a level of security appropriate to the risk, it merely provides a brief list of strategies to be included 'inter alia as appropriate'. By contrast, Article 29 LED introduces a total of eleven specific guarantees and forms of information control that must be ensured through the adoption of safety measures. Among others, these requirements make direct mention of storage control, equipment access control, data media control, communication control, transport control, recovery, integrity and reliability. Given the particularly sensitive nature of the data that law enforcement agencies and criminal justice authorities frequently process, these stringent and detailed security conditions are a welcome addition to the LED.

Second, mention deserves to be made of the extent to which this article corresponds to the strategies and principles established in the field of cyber- and information security. In this sphere, ensuring a high level of security is widely considered to necessitate compliance with the so-called CIA-triad that the emphasises the importance of the Confidentiality, Integrity and Availability of computer systems and

---

[435] For further analysis of the possible scope and nature of these mitigation measures in the context of law enforcement, see: Bas Seyyar, M. and Geradts, Z.J.M.H., 'Privacy impact assessment in large-scale digital forensic investigations', Forensic Science International: Digital Investigation, Vol. 33, 2020; Marquenie T. and Quezada-Tavárez K., 'Data Protection Impact Assessments in Law Enforcement: Identifying and Mitigating Risks in Algorithmic Policing' in Markarian G., Nitsch H., Karlovic R. & Chandramouli, K. (eds), *Security technologies and social implications: An European Perspective*, Wiley-IEEE Press, 2022 (under review).

[436] Art. 7 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Strasbourg, 28.01.1981 ('Convention 108').

[437] Art. 4(1)(f) LED and Art. 5(1)(f) GDPR.

the data therein.[438] Under the principle of Confidentiality, the data is only to be accessible by individuals with the proper credentials and authorisations. The concept of Integrity necessitates that the data must be maintained in a manner that is reliable, accurate and complete, and the notion of Availability requires that the data is accessible by the desired individuals when needed. When considering how these principles are reflected in the LED, a critical concern must first be raised as the primary goal of data protection law appears to diverge from the main objective of information security. In practice, both fields attempt to achieve the same purpose, which is to protect the data and processing systems from undue use or interference that risks altering, removing or revealing their contents to unauthorised individuals. Their motivations behind this, however, tend to differ.[439] From an information security perspective, the primary goal of securing the data typically is to protect the interests of the controller from a loss of revenue, information or confidential information. By contrast, security requirements under data protection law principally aim to safeguard the rights and freedoms of the data subject whose personal information is compromised and put at risk. Yet despite these divergent motivations, it appears that little cause for concern remains when evaluating the adherence to the basic tenets of information security in the LED. The components of Article 29 provide a robust framework that incorporates high security standards and fully reflects the fundamental principles of cybersecurity.[440]

When examining various national implementations of this provision, it appears that Member States have taken a variety of different approaches towards data security. Some countries, like Belgium and Ireland[441], have closely adhered to the structure of Article 29 LED and contain an equally extensive list of specific security measures to be taken. Others have not only instituted the same conditions but opted to go beyond the minimum requirements of the LED by introducing further guarantees for data security. Germany, for example, also mandates that competent authorities ensure that data collected for different purposes is able to be processed separately ('separability') and that processing operations taking place on behalf of the controller can only occur in compliance with the controller's instructions ('processing control').[442] **However, not all Member States have incorporated such a degree of detail into their national provisions.** The Netherlands, for instance, appears to have integrated the obligation of data security into its expanded stipulations regarding data protection by design.[443] In doing so, it foregoes providing a list of specific methods of security controls but instead presents more general requirements concerning the security of processing and compliance with data protection principles, such as by mandating that the appropriate technical and organisational measures must ensure a fitting level of security by protecting police data against unauthorised or unlawful processing and intentional loss, erasure or damages. Naturally, safety concerns necessitate that information regarding the internal implementation of security measures is rarely made public, thus making it difficult to assess the actual level of data security maintained by competent authorities. Nevertheless,

[438] European Union Agency for Network and Information Security (ENISA), 'Guidelines for SMEs on the Security of Personal Data Processing', 2016.

[439] Ripoll Servent, A., 'Protecting or Processing? Recasting EU Data Protection Norms' in Schünemann, W.J. and Baumann, M.O., (eds), *Privacy, Data Protection and Cybersecurity in Europe*, Springer 2017.

[440] For an extensive examination of this topic, see: Marquenie, T. and Quezada-Tavárez, K., 'Operationalization of Information Security through Compliance with Directive 2016/680 in Law Enforcement Technology and Practice' in Vedder, A., Schroers, J., Ducuing, C. and Valcke, P. (eds), *Security and Law*, Intersentia, 2019.

[441] Art. 60 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018) and Art. 70 Data Protection Act 2018 (Act 7 of 2018) (Iris Oifigiúl 42 p. 00752, 24 May 2018).

[442] Art. 64 Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).

[443] Art. 4a Wet van 21 juli 2007 houdende regels inzake de verwerking van politiegegevens (Wet Politiegegevens, Stb. 2007, 549).

the standards introduced by the LED and the national laws based thereon appear to instate a robust framework of information security that closely reflects existing practices in the field of cybersecurity.

Regarding Articles 30 and 31, a brief remark can also be made about the practical application of the procedures surrounding the reporting of data breaches. Although the transposition of these provisions into national law appears to have been generally uniform, the actual interpretation thereof seems to reflect some notable differences in national practice. As indicated in the European Commission's report, there exist significant disparities in the number of reported data breaches. While several supervisory authorities reported no notifications, others received hundreds of notices. Such a large discrepancy led to the conclusion that there likely exist divergent interpretations of what constitutes a data breach and when they should be reported to the supervisory authority.[444] In line with the Commission's findings, it is thus recommended that a more uniform approach to the management of data breaches ought to be taken.[445]

[444] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 20.

[445] As noted by the Commission, the EDPB's recent guidelines on personal data breach notifications can prove a valuable source of guidance to this end. For more, see: European Data Protection Board, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Adopted on 14 December 2021, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf

6. DATA TRANSFERS TO THIRD COUNTRIES

KEY FINDINGS

The lack of adequacy decisions under Article 36 LED and the possible difficulties in detaching them from the GDPR's divergent scope and considerations risks undermining a cornerstone of international transfers by competent authorities and weakening the protection of EU fundamental rights beyond the Union's borders. It is recommended that the adoption of additional adequacy decisions is prioritized further.

The continued reliance on legally binding instruments that were adopted before the EU data protection reforms and are therefore unlikely to be in compliance with current norms stands to be to the detriment of the high level of EU data protection guarantees and undermine the protection of EU fundamental rights in international transfers. Additionally, Article 37 LED assigning competent authorities with the responsibility of assessing whether 'appropriate safeguards' that provide in an 'essentially equivalent' level of data protection are in place poses serious threats to a consistent and robust framework of transfers that provides in adequate protection for the rights of EU data subjects, thus indicating that further action may be warranted to align national standards.

Concerns have been raised regarding the interpretation of Article 39 LED on the transfers to private entities in third countries, as diverging perspectives exist on its place in the structure of Chapter V. In addition, national implementations of this, albeit optional, provision appear difficult, and there is little consistency among EU legal instruments regarding such transfers.

6.1 General

Chapter V of the Directive concerns the transfers of personal data to third countries or international organisations. As an important objective of EU data protection law is to protect the rights and interests of European data subjects even beyond its borders, transfers to competent authorities located in third countries must comply with certain conditions and be covered by adequate safeguards in order to be lawful. To this end, Article 35 establishes the general principles for these transfers. Principally, it stipulates that they can only take place between competent authorities, are not to undermine the general level of protection provided by the Directive, and must be necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding of public security. Furthermore, the provision mimics the general architecture of the GDPR and establishes a three-step cascading approach to the transmission of personal data outside of the EU. In accordance with this cascade, these transfers may only take place when the European Commission has issued an adequacy decision authorising transfers to a country that ensures an adequate level of data protection, or, in absence of such a decision, appropriate safeguards exist with regards to the protection of personal data, or, in absence of such safeguards, certain derogations for specific situations apply. In addition, Chapter V also provides in the possibility of transferring personal data directly to non-competent recipients in third countries when certain conditions are met.

In regulating the exchange of personal data beyond the borders of the EU, this Chapter seeks to strike a delicate balance between different interests.[446] On the one hand, the legal framework for international transfers has to take into account the particularities of data processing in the context of law enforcement and criminal justice. As the cooperation with competent authorities in third countries is often paramount to the effective functioning of European law enforcement, the data protection rules must provide in a certain flexibility and meet the unique needs of police and criminal justice actors. On the other, the significant risks associated with international transfers and the inherent limits to oversight once personal data leaves the EU territory mandates robust and enforceable safeguards to protect the rights and interests of data subjects. If found to be overly permissive, the current approach to such transfers risks eroding the protection of personal data and human rights by granting the competent authorities too much discretion.[447] The following section examines several key aspects of Chapter V and highlights a number of outstanding concerns.

6.2 Adequacy decisions

Constituting the first step in the abovementioned cascade, adequacy decisions serve as a prominent and formal assurance of the existence of robust data protection standards for data transfers to third countries.[448] As stipulated by Article 36, such assessments are to take into account various elements such as the adherence to human rights, the existence of local data protection rules, the effective functioning of supervisory authorities, and the observance of international commitments. By relying on a single institution that is well-equipped to assess the level of data protection observed in foreign territories, the issuance of adequacy decisions by the European Commission is likely to result in a more consistent application of the LED and its principles. These decisions have the potential of being a particularly effective measure for the transfer of personal data to third countries in a legally sound and human rights compliant manner.[449] While they play an important role in enabling European competent authorities to engage in sustained cooperation with operational partners in third countries, a number of concerns can nevertheless be raised regarding the current approach to adequacy decisions under the LED.

First, **the relatively low frequency at which these decisions are issued stands to limit the efficacy of this cornerstone provision.** While the European Commission has issued over a dozen adequacy decisions under Directive 95/46 EC and the GDPR, it has only recognised a single third country as providing an adequate level of data protection for transfers in the context of law enforcement. This

[446] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology,* Vol. 33, No 3, 2019, pp. 249–270.

[447] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

[448] European Data Protection Board, Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, 2 February 2021.

[449] Drechsler, L., 'Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context', *International Data Privacy Law*, Vol. 11, No. 2, 2021, pp. 182-195.

decision[450] applies to the EU's post-Brexit relationship with the United Kingdom[451] and was adopted in June 2021.[452] Consequently, it remains up to the Member States and their individual competent authorities to bear the responsibility of determining whether appropriate safeguards or derogations for specific situations warrant the transfers of data to any third country other than the United Kingdom. This risks introducing a significant degree of legal uncertainty and result in a lack of consistency if competent authorities within the EU take a divergent approach to the evaluation of the circumstances of international data transfers. As a result, data protection experts have indicated that the existence of LED adequacy decisions is of crucial importance to safeguard EU fundamental rights and protect the interests of European data subjects beyond the Union's borders.[453]

The lack of adequacy decisions also stands to disproportionately affect Member States that have a particular relationship with their autonomous territories. For example, the Kingdoms of both Denmark and the Netherlands consist of overseas regions that are not part of the EU themselves.[454] Given that these areas are considered to be third countries, data transfers between these countries and their territories will be subject to the framework established in Chapter V of the LED. In the current absence of adequacy decisions validating enduring exchanges of personal data between these entities, the Dutch and Danish competent authorities are required to continuously assess whether appropriate safeguards warrant the transfer of data to law enforcement agencies and criminal justice authorities belonging to the same country. This situation can be experienced as cumbersome and has been perceived as inhibiting the effective cooperation between competent authorities.[455]

Accordingly, **it is recommended that the Commission places further emphasis on the adoption of adequacy decisions under the LED**.[456] As further discussed below, serious issues are associated with leaving the assessment of equivalent data protection standards in third countries up to the discretion of competent authorities that are likely to lack the resources and expertise of the Commission. Given

---

[450] In this context, it deserves mention that the UK adequacy decisions have not gone without criticism. While limiting their commentary to the decision under the GDPR, scholars have previously raised concerns regarding onwards transfers, oversight, surveillance and alignment with CJEU case law. However, given the similarities between the adequacy decisions under the GDPR and LED, it remains possible that similar issues might arise during the application, monitoring or review of this decision. For more, see: Korff, D. and Brown, I., 'The inadequacy of UK data protection law. Part one: General Inadequacy', 9 October 2020; Korff, D. and Brown, I., 'The inadequacy of UK data protection law. Part two: UK surveillance', 30 November 2020.

[451] Regarding this adequacy decision, brief note must be made of the LIBE Committee's suggestion that further clarity is provided on how the UK's future alignment with EU data protection standards will be monitored. See: Chairman of Committee on Civil Liberties, Justice and Home Affairs, 'LIBE Contribution to the Commission upcoming report on the evaluation and review of the Law Enforcement Directive', IPOL-COM-LIBE D (2022)3535, 7 February 2022.

[452] Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4801, Brussels.

[453] Drechsler, L., 'Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context', *International Data Privacy Law*, Vol. 11, No. 2, 2021, pp. 182-195.

[454] Denmark has such a relation with the Faroe Islands and Greenland. The Netherlands has a comparable relationship with Aruba, Curaçao, Sint Maarten and the Caribbean Netherlands. For more, see: Stephan S., 'Greenland, the Faroes and Åland in Nordic and European Co-operation – Two Approaches towards Accommodating Autonomies', *International Journal on Minority and Group Rights,* Vol. 24, No. 3, 2017; Broekhuijse I., Ballin E.H. and Ranchordás S., 'The Constitutions of the Dutch Caribbean: A Study of the Countries of Aruba, Curaçao and Sint Maarten and the Public Entities of Bonaire, Sint Eustatius and Saba' in Albert R., O'Brien D. and Wheatle S. (eds.), *The Oxford Handbook of Caribbean Constitutions*, Oxford University Press 2020.

[455] Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, 2020.

[456] This recommendation is shared by the Chairman of the LIBE Committee. See: Chairman of Committee on Civil Liberties, Justice and Home Affairs, 'LIBE Contribution to the Commission upcoming report on the evaluation and review of the Law Enforcement Directive', IPOL-COM-LIBE D (2022)3535, 7 February 2022.

that adequacy decisions are well-suited as the primary cornerstone of a consistent framework for third country transfers of police data, it is highly advisable that the Commission provides further insight into the process of issuing such decisions and takes steps to expedite their future adoption. Providentially, it appears that the Commission shares this intent. In its recent report on the LED, the Commission notes that it is "actively promoting the possibility of adequacy findings with other key international partners" and "will […] consider other possible candidates for future adequacy decisions under the LED", citing the recent adoption of the Directive and the ongoing global convergence of data protection rules in law enforcement as reasons behind the low number of current adequacy decisions.[457]

Second, note must be made of the apparent disparities between adequacy decisions pursuant to the GDPR and the LED. Considering the differences between both instruments and the separate contexts in which they aim to safeguard the rights and interests of data subjects, it has been argued that decisions under the LED cannot simply be modelled on their GDPR counterparts and that prior assertions by the Commission[458] may be misguided in positing that the latter can act as a basis for assessments concerning the law enforcement sector.[459] This primarily stems from the inclusion of certain freedoms in the LED that are not explicitly protected by the GDPR[460] and might necessitate a different consideration of which data protection standards constitute as adequate, as well as from the additional limits placed on the competences and independence of independent supervisory authorities and the exercise of data subject rights to access and information. According to the European Data Protection Board (EDPB), this also signifies that the assessment must take into account data protection rules that apply specifically to the field of law enforcement, as genera data protection standards are insufficient to cover police processing activities.[461]

In this context, the unique nature of the LED must be duly considered in light of recent case law on adequacy decisions and third country transfers.[462] In the Schrems case, the CJEU established that a third country must provide in an 'essentially equivalent' level of protection of fundamental rights and freedoms in order to be considered adequate.[463] In relation to the Safe Harbour framework for transfers with the United States, the Court noted that American authorities were able to access and process data beyond the agreement's protective rules and limitations, and that the framework did not provide in sufficient opportunity for data subjects to obtain redress or pursue legal remedy. While this judgment was issued in the context of a decision issued under the GDPR, the EDPS and WP29 have subsequently

[457] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, pp. 26-27.

[458] Commission Expert Group, 'Minutes of the seventh meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680', Commission Expert Group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (DPR), 7 March 2017.

[459] Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', *Global Privacy Law Review*, Vol 1, No. 2, 2020, pp. 93–103.

[460] Consider, for example, the right of presumption of innocence in criminal proceedings as mentioned by Recital 31 of the LED and safeguarded by Article 48 of the EU Charter of Fundamental Rights.

[461] European Data Protection Board, Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, 2 February 2021.

[462] For a comprehensive overview of this matter, see: Drechsler, L. and Kamara, I., 'Essential equivalence as a benchmark for international data transfers after Schrems II' in Kosta E. and Leenes R. (Eds.), *Research handbook on EU data protection*, Edward Elgar 2022.

[463] Judgment of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner,* Case C-362/14, ECLI:EU:C:2015:650.

noted its relevance for the LED.[464] Similarly, the CJEU Opinion 1/15 on the EU-Canada PNR Agreement[465] reaffirmed that the mere act of transferring personal data to a third country results in an interference with the rights to privacy and data protection, thus necessitating that appropriate safeguards and enforcement mechanisms apply to the transfers and, among others, relate to the existence of independent supervision and limitations on the extent of the data processing.[466] These requirements were further developed in the Schrems II case[467] that stressed the importance of proportionality and effective protections against abuse, and that mandated the application of clear and precise rules that limit the transfers to what is strictly necessary.[468] In a similar fashion to Schrems I, the CJEU made particular reference to the lacking Ombudsperson mechanism for judicial protection of EU data subjects and the insufficient restrictions on the broad use of and access to personal data of EU citizens.

As such, the European Commission must exercise caution and consider these fundamental differences with the GDPR when examining the adequacy of third country data protection standards in the sphere of law enforcement. To this end, the EDPB's guidance on LED adequacy decisions provides further, albeit limited[469], insight into how certain provisions might be reflected by data protection legislation in third countries.[470] It is paramount that the standard of essential equivalence is considered through the lens of policing and criminal justice by taking into account the impact third country transfers might have on rights and freedoms that are not typically considered in a data protection context. This holds particularly true if foreign competent authorities utilise expansive technologies such as those that involve profiling, tracking, big data, facial recognition and predictive analytics due to their high likelihood of infringing upon various fundamental rights and the proportionality of criminal investigations and sentencing.[471] **Given these particular challenges posed by data transfers in a law enforcement context, legal scholarship has noted that 'uncoupling of LED adequacy decision from GDPR adequacy decisions would be crucial' to guarantee the protection of various EU fundamental rights in certain cases**.[472]

---

[464] European Data Protection Supervisor, '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', 28 October 2015; 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 or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', WP 233, 1 December 2015.

[465] Judgment of 26 July 2017, *Case Opinion 1/15 of the Court (Grand Chamber)*, ECLI:EU:C:2017:592.

[466] Brouwer, E., 'Private Life and Data Protection in the Area of Freedom, Security and Justice' in Iglesias Sánchez S. and González Pascual M. (eds), *Fundamental Rights in the EU Area of Freedom, Security and Justice*, Cambridge University Press, 2021.

[467] Judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland and Schrems*, Case C-311/18, ECLI:EU:C:2020:559.

[468] For a thorough examination of the relevant case law and its consequences, see: Brown, I. and Korff, D., 'Exchanges of Personal Data After the Schrems II Judgment', European Parliament Committee on Civil Liberties (LIBE), July 2021.

[469] Drechsler, L., 'EDPB Issues Guidance on Personal Data Transfers Based on Adequacy Decisions in the Context of the Law Enforcement Directive', *European Data Protection Law Review*, Vol. 7, No. 2, 2021.

[470] European Data Protection Board, Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, 2 February 2021.

[471] For example, the CJE has noted that technologies enabling the real-time collection of data that allows for the tracking of individuals' movements constitute a particularly serious interference with human rights. See: Judgment of 6 October 2020, *La Quadrature du Net and Others,* C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 92.

[472] Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', *Global Privacy Law Review*, Vol 1, No. 2, 2020, pp. 93–103.

6.3 Appropriate safeguards and specific derogations

In absence of an adequacy decision, competent authorities can still transfer personal data to third countries when appropriate safeguards are in place or, lacking such safeguards, if certain derogations for specific situations apply. Pursuant to Article 37, the appropriate safeguards can be provided for in a legally binding instruments or deemed to exist by the transferring authority following an assessment of the circumstances. Under Article 38, competent authorities can derogate from the requirement of an adequacy decision or appropriate safeguards and transfer personal data when certain conditions are met. This is only possible when the transfer is deemed necessary to protect specific interests of the data subject, prevent an immediate and serious threat to public security, or in individual cases relating to purposes set out in Article 1(1) when the rights of the data subject do not override the public interests at hand.[473]

In practice, the appropriate safeguards in Article 37 serve as the default ground for most transfers outside of the EU given the derogations' more limited scope of application and the abovementioned lack of adequacy decisions.[474] Consequently, they are vital in enabling the international cooperation between EU and foreign competent authorities, and fulfil an important role in upholding the LED's high data protection standards for data exchanges with third countries. [475] Yet, despite their critical function, a number of remarks are in order.

First, the continued reliance on legally binding instruments that were adopted before the conclusion of the EU data protection reforms stands to undermine the current level of data protection. Following Article 61 LED, previously concluded international agreements are allowed to remain in force until amended, replaced or revoked. As further clarified by Recital 71 LED, this includes 'legally binding bilateral agreements' on the basis of which Member States engage in direct cooperation with law enforcement agencies abroad.[476] This poses a clear risk concerning the potential inadequacy of data protection standards provided for in these instruments. If Member States continue to exchange confidential and sensitive police data on the basis of agreements that may have been concluded decades before the modern standards established by the LED, it seems unlikely that European data

[473] As noted by the European Commission, there does not currently exist guidance for the transfers of personal data by means of these derogations. This is contrast with the situation under the GDPR, for which there do appear to exist guidelines on the equivalent procedure under Article 49 of the Regulation. For more, see: European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 32.

[474] Drechsler, L., 'The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive', *Cybercrime: New Threats, New Responses - Proceedings of the XVth International Conference on Internet, Law & Politics*, Barcelona, 1-2 July, Huygens Editorial 2020.

[475] In this context, reference ought to be made to the ongoing negotiations for a cooperation agreement between the EU and Interpol. Seeking to enhance the exchange of information between Interpol and various EU institutions, such an agreement must ensure that Interpol provides in an equivalent level of data protection to allow for data transfers thereto to occur. To this end, considerations must be made of Interpol's policies on data processing and data protection, as well as of safeguards against potentially problematic exchanges of data such as those relating to politically motivated red notices as discussed previously under Section 3.5. For more, see: European Data Protection Supervisor, 'Opinion 8/2021 on the Recommendation for a Council decision authorising the opening of negotiations for a cooperation agreement between the EU and INTERPOL', 25 May 2021; Wandall, R., Ensuring the rights of EU citizens against politically motivated Red Notices', European Parliament Committee on Civil Liberties (LIBE), February 2022; European Parliament, 'European Parliament recommendation of 5 July 2022 to the Council and the Commission on the negotiations for a cooperation agreement between the European Union and the International Criminal Police Organization (ICPO-INTERPOL)', 2022/2025(INI), 5 July 2022.

[476] As noted by Drechsler, a key example of such an agreement is the Mutual Legal Assistance Treaty (MLAT) that underlies most international data exchanges between competent authorities. See: Drechsler, L., 'Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context', *International Data Privacy Law*, Vol. 11, No. 2, 2021, pp. 182-195.

subjects' rights and freedoms are adequately protected during these exchanges.[477] While Article 37 and Recital 71 nevertheless stress that these legal instruments are still to provide an adequate level of data protection, **there appears to exist little motivation or scrutiny to ensure that these standards are met, despite substantial evidence that these agreements likely contain insufficiently strong safeguards.**

To illustrate this, one can refer to the efforts by the European Commission to review these international agreements and establish whether they are consistent with the contemporary EU data protection regime. For instance, the Commission issued a recent Communication in which it determined that ten EU legal acts in the AFSJ must be amended and brought in line with the LED[478], and its evaluation of the data protection standards in Europol's international cooperation agreements is currently ongoing.[479]

Similarly, the Mutual Legal Assistance Treaty between the EU and USA was revised by the so-called Umbrella Agreement of 2016[480] which introduced stronger data protection rules to meet the current European standards.[481] While the CEG acknowledged this issue and accepted that some agreements might conflict with the Directive[482], it noted a degree of flexibility in addressing the problem and asserted that Member States are to 'map the existing situation' and independently explore solutions such as additional protocols or an 'interpretative understanding' of the instruments. The fact that Member States are thus merely requested but not immediately obliged to amend these texts thus risks undermining a cornerstone of the rules concerning international data transfers.[483] It is with this risk in mind that the European Data Protection Board has recently issued a statement in which it invites Member States to "assess and, where necessary, review their international agreements that involve international transfers of personal data" for the purpose of determining whether further alignment with Union legislation, case law and EDPB guidance might be warranted.[484] In line with the European

---

[477] Drechsler, L., 'The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive', *Cybercrime: New Threats, New Responses - Proceedings of the XVth International Conference on Internet, Law & Politics*, Barcelona, 1-2 July, Huygens Editorial 2020.

[478] Communication from the Commission to the European Parliament and the Council, 'Way forward on aligning the former third pillar acquis with data protection rules', COM(2020) 262, Brussels, 24 June 2020.

[479] For a more extensive overview of the Commission's efforts in this context, including the negotiations on a Second Additional Protocol to the Cybercrime Convention, the process of amending the mutual legal assistance treaty between the EU and Japan, and the negotiations on an agreement with the United States regarding the cross-border access of electronic evidence, see: European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 28.

[480] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, OJ 2016 L 336/3.

[481] As noted by the European Commission, this Agreement and its implementation is currently the subject of a joint review. For more, see: Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, pp. 28-29.

[482] Commission Expert Group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (DPR), 'Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680', 4 May 2017.

[483] Di Francesco Maesa, C., 'Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)', *Eurojus Italia*, 24 May 2016, http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/.

[484] European Data Protection Board, Statement 04/2021 on international agreements including transfers, Adopted on 13 April 2021, https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf

Commission's recommendations[485], it is nevertheless advisable that the EDPB provides additional guidance and concrete instructions for the execution of an adequacy self-assessment by national authorities.

At present, **seemingly little urgency has been ascribed to the situation as no substantial steps appear to have been taken to align these agreements with the LED**.[486] Given that WP29 has previously criticised the LED for lacking an explicit requirement that Member States amend such outdated instruments[487], it seems almost inevitable that this problem will persist in absence of further intervention. A more extensive examination of this issue resulting in concrete guidance at the European level and renewed focus on aligning existing instruments with contemporary standards may thus be in order.

Second, concerns must be raised regarding the interpretation of the concept of appropriate safeguards. In Schrems II, the CJEU affirmed that these safeguards are required to meet the same standard of 'essential equivalence' that the Commission's adequacy decisions are expected to establish.[488] As mentioned above, this notion has been developed in EU case law and signifies that the legal framework of third countries must reflect the 'core requirements' of EU data protection legislation by providing functionally equal safeguards in order to be considered as providing an adequate level of protection.[489] While holding the appropriate safeguards to the same standard as adequacy decisions deserves praise for upholding a consistently high level of data protection for the most common forms of international data transfers, **this stipulation nevertheless risks introducing a significant degree of legal uncertainty that stands to affect the efficacy of Article 37 of the LED.**[490] This uncertainty stems from it being the responsibility of the transferring competent authority to conduct a self-assessment of the circumstances and determine whether the applicable safeguards meet the threshold of adequacy and essential equivalence. Given the lack of concrete guidance on how this assessment should be conducted[491], such an approach to international transfers places a significant burden on EU competent authorities and risks leaving the underlying issues unaddressed.[492] In addition to fulfilling their law enforcement mandate and investigating criminal offenses, these agencies are now tasked

---

485 European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 32.

486 Marquenie, T., 'Article 39: Transfers of personal data to recipients established in third countries' in Kosta, E. and Boehm, F. (eds), *The Law Enforcement Directive: A Commentary*, Oxford University Press 2022 (forthcoming – under review).

487 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 purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', WP 233, 1 December 2015.

488 Judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland and Schrems*, Case C-311/18, ECLI:EU:C:2020:559, para. 96.

489 European Data Protection Board, 'Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive', 2 February 2021.

490 Drechsler, L., 'EDPB Issues Guidance on Personal Data Transfers Based on Adequacy Decisions in the Context of the Law Enforcement Directive', *European Data Protection Law Review*, Vol. 7, No. 2, 2021.

491 The EDPB has only provided such guidance in the context of the GDPR. While this might provide some relevant information, it is not suited for the particularities of the LED and cannot be considered sufficiently applicable. See: European Data Protection Board, 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures', 10 November 2020.

492 Domingo Sanchez, M.B., 'The protection of personal data in the area of freedom, security and justice: special consideration of data transfers to third countries and international organizations according to directive 2016/680', *Revista de Estudios Europeos*, No. 69, 2017.

with the daunting challenge of addressing complex issues of international law, data protection and human rights.

When considered alongside the previous point on the potential flaws in prior international agreements, this outcome has been described by some scholars as the 'Achilles heel' of contemporary data protection law in the context of law enforcement.[493] The extent of the challenge faced by the competent authorities is further illustrated by recent case law. In the abovementioned judgements of Schrems I and Schrems II as well as Opinion 1/15, the CJEU has previously invalidated several decisions made by the European Commission over shortcomings in its assessments.[494] Requiring national or local competent authorities with considerably less resources, time and expertise on legal manners to reliably and accurately assess the level of protection offered by third countries thus poses a serious threat to the integrity of the EU data protection framework. While the LED only contains an explicit requirement for the Commission to assess the "respect for human rights and fundamental freedoms" when issuing adequacy decisions for third countries, some subject matter experts have argued that the Schrems II judgement entails that all transfer mechanisms ought to ascertain that an equivalent level of protection for human rights beyond just data protection is in place.[495] Such a situation might thus compel national competent authorities and, to the extent that they are involved, supervisory authorities to consider highly complex matters relating not just to policing and law enforcement but the exercise of and respect for fundamental freedoms in foreign legal systems.[496]

Without clear guidance and a more extensive framework of adequacy decisions[497], it appears inevitable that Article 37 will be subject to diverging interpretations among Member States and thus result in an inconsistent application of the LED, as it appears likely that competent authorities might transmit personal data to third countries that do not provide in safeguards that would be considered sufficiently strong by all Member States or European institutions. **Given that such a situation would inevitably be to the detriment of legal certainty and the EU human rights and fundamental freedoms, further action may be needed to address these issues and provide additional clarity on the assessment of human rights standards for third country transfers. Further examination of the**

---

493 Drechsler, L., 'The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive', *Cybercrime: New Threats, New Responses - Proceedings of the XVth International Conference on Internet, Law & Politics*, Barcelona, 1-2 July, Huygens Editorial 2020.

494 In this context, it must be noted that other EU institutions such as the European Parliament had previously voiced concerns about the safeguarding of certain European rights through these adequacy decisions and had already called for further action to be taken before these legal proceedings and the intervention by the CJEU. For more, see: Brown, I. and Korff, D., 'Exchanges of Personal Data After the Schrems II Judgment', European Parliament Committee on Civil Liberties (LIBE), July 2021.

495 Drechsler, L., 'The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive', *Cybercrime: New Threats, New Responses - Proceedings of the XVth International Conference on Internet, Law & Politics*, Barcelona, 1-2 July, Huygens Editorial 2020.

496 As a matter of illustration, reference can be made to the current invasion of Ukraine by the Russian Federation. As noted in a recent statement by the European Data Protection Board, data exporters and supervisory authorities are expected to monitor ongoing developments in Russia and determine whether they might interference with the effectiveness of the appropriate safeguards and warrant the suspension of such transfers. While the statement refers to transfers under the GDPR and the Board neither appeared to consider the ongoing conflict as a reason to categorically suspend all transfers to Russia nor examine the impact of potential human rights violations on these exchanges of data, the situation is nevertheless indicative of the difficult balance that competent authorities may have to strike when considering if adequate safeguards exist to allow for data transfers to third countries. For reference, see: European Data Protection Board, 'Statement 02/2022 on personal data transfers to the Russian Federation', 12 July 2022.

497 As summarized by Drechsler, the LED's other options for third country transfers 'reveal significant drawbacks when compared to a potential LED adequacy decision in terms of the fundamental rights protection offered'. See: Drechsler, L., 'Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context', *International Data Privacy Law*, Vol. 11, No. 2, 2021, pp. 182-195.

desired responsibilities held by competent authorities as well as the role played therein by supervisory authorities may thus be in order.

6.4 Transfers to private recipients and non-police bodies

As a general rule, competent authorities are to limit transfers of personal data to recipients with a law enforcement or criminal justice mandate of their own.[498] This is due to the often sensitive and highly confidential nature of police data precluding their exchange with private entities or non-police public bodies. With regards to international transfers, this principle had previously been affirmed by various legal instruments and data protection bodies[499] before being cemented in Article 35(1)(b) of the LED. In exceptional situations, however, competent authorities might determine that sharing personal data with non-competent recipients in third countries is necessitated by an overriding public interest that warrants the interference with a data subject's rights to avert an imminent threat or respond to a criminal offence. It is in this context that Article 39 LED lays out the general framework for these asymmetrical transfers and establishes minimum standards for the Member States that allow their competent authorities to engage in such exchanges of data. These transmissions are only lawful when necessary to avert an imminent threat or respond to a criminal offence, and when it would be ineffective or inappropriate to transfer the data to a local competent authority instead. As such, this provision might be particularly useful for the urgent collaboration with foreign service providers to preserve digital evidence or intervene against ongoing instances of cybercrime and human trafficking.

Considered by some to be 'the most innovative provision' of the Chapter[500], this article introduces an important set of rules for an atypical kind of data transfers that might otherwise circumvent the high level of data protection in the LED. Regardless, certain aspects of the provision and the national implementation thereof raise both legal and practical questions on its scope and use.

First, **there exists some uncertainty as to how Article 39 relates to the three-step structure established in Articles 35 to 38.** Since Article 39 only mentions an explicit deviation from the abovementioned principle in Article 35(1)(b), some scholarship has suggested that the lack of a similar derogation from Article 35(1)(d) indicates that transfers to non-competent recipients must still be based on an adequacy decision, appropriate safeguards or derogation for specific situations.[501] Other literature, however, has posited that these transmissions constitute a specifically regulated exception to adequacy decisions[502] and, moreover, that such an interpretation is difficult to reconcile with the time-sensitive nature of Article 39 and would result in a 'disjointed reading' of Chapter V.[503]

Further arguments raised to support an interpretation of this provision as distinct from the three-step cascade include the possibility of applying Article 39 to transfers to third countries even when they fail

---

[498] Boulet, G. and De Hert, P., 'Cooperation between the private sector and law enforcement agencies: an area in between legal regulations', in Aden H. (ed.), *Police Cooperation in the European Union under the Treaty of Lisbon - Opportunities and Limitations*, Nomos Verlagsgesellschaft 2015.

[499] Principle 5 of the Council of Europe Recommendation No. R (87) 15 regulating the use of personal data in the police sector, 17 September 1987; 'Position Paper on Law Enforcement and Information Exchange in the EU', *Spring Conference of European Data Protection Authorities*, Krakow, 25-26 April 2005; European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM(2005)475, 2006.

[500] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

[501] Ibid.

[502] Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', *Global Privacy Law Review*, Vol 1, No. 2, 2020, pp. 93–103.

[503] Marquenie, T., 'Article 39: Transfers of personal data to recipients established in third countries' in Kosta, E. and Boehm, F. (eds), *The Law Enforcement Directive: A Commentary*, Oxford University Press 2022 (forthcoming – under review).

to respect the rule of law, which might complicate the reliance on an adequacy decision or appropriate safeguards, and the potential issues faced when attempting to align or combine the set of conditions for derogations under Article 38 with those in Article 39. Additionally, Article 39 is the sole provision relating to international transfers mandating that its application is without prejudice to international agreements, thus further separating itself from the other provisions in its relationship with such protocols, and a preparatory document by the Council appears to distinguish transfers under this article from those that take place "on the basis of" Articles 37 and 38, thereby indicating that they may exist independently of each other.

Similarly, concerns have been raised regarding the applicability of Article 39 to the involvement of processors in third countries. Article 35 (1)(b) asserts that personal data may only be transmitted to recipients that take on the role of a data *controller*. Following a strict reading of this provision, transfers to third country *processors* would either be prohibited in their entirety or, depending on the chosen interpretation of the previous paragraph, only exceptionally possible under Article 39. Given this provision's narrow scope of application and strict conditions, it is highly questionable that Article 39 would be suitable to cover this type of cooperation.[504] However, it appears that such a strict reading might be unintended as Recital 64 appears to suggest that transfers to processors in third countries can be lawful when the level of data protection established by the LED is preserved**.**

While both interpretations raise valid arguments, it appears preferable and arguably more convincing to interpret Article 39 as providing in its own basis for transfers and not requiring that the transfers thereunder are simultaneously grounded in the other mechanisms of Chapter V. Nevertheless, **further clarification on this matter as well as the relationship between Article 39 and the three-step architecture would be welcome.**

Second, the abovementioned concerns regarding the continued utilisation of pre-existing international agreements are equally relevant in the context of this provision. As Article 39(1) LED explicitly notes that these transfers are to occur 'without prejudice to any international agreement referred to in paragraph 2 of this Article'[505], previously concluded arrangements and treaties on police cooperation are to remain in force and must be adhered to when relevant to such transfers. This means that the aforementioned risk of data transfers taking place on the basis of instruments that are not in line with modern data protection standards and fail to provide adequate safeguards for the rights of the individuals persists in relation to Article 39 LED as well.[506]

Third, attention must be brought to a possible issue surrounding the national implementation of this provision. As illustrated by the use of the word 'may' and further confirmed by the CEG[507], Article 39 does not impose an obligation to allow for third country transfers to non-competent recipients. Instead, it merely provides a set of minimum standards in the event that Member States would permit their competent authorities to engage in such transmissions. Yet while optional in nature, this could

---

[504] Drechsler, L., 'Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context', *International Data Privacy Law*, Vol. 11, No. 2, 2021, pp. 182-195.

[505] Article 39(2) clarifies that these agreements 'shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation'.

[506] It is thus recommended that the Commission adheres to the LIBE Committee's request to provide further details on which agreements have been assessed and, subsequently, amended, replaced or revoked. See: Chairman of Committee on Civil Liberties, Justice and Home Affairs, 'LIBE Contribution to the Commission upcoming report on the evaluation and review of the Law Enforcement Directive', IPOL-COM-LIBE D (2022)3535, 7 February 2022.

[507] Commission Expert Group, 'Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680', 7 November 2016.

nevertheless introduce uncertainty surrounding the existence of a national legal basis.[508] As several Member States have transposed the LED by including its provisions in a standalone data protection law, the mere implementation of Article 39 in national law does not necessarily establish a legal basis for these transfers by its own right. Generally speaking, it is legislation on the functioning of police and the management of law enforcement data that provides the appropriate legal basis by determining the specific circumstances and recipients of international data transfers.[509] Without making the necessary amendments to these instruments, Member States thus risk leaving this aspect of their data protection legislation as functionally void. An example of this may be found in Belgium where Article 70 of its national Data Protection Act[510] duly incorporates the conditions of Article 39 LED but the corresponding Act on the Police Service[511] has not been amended to provide an actual legal basis that allows for these transfers to occur. Accordingly, this provision is rendered inoperable in practice and stipulates requirements for transmissions that remain unlawful without further legislative interventions. **While the legal implications of such a situation are likely to be limited due to the optional nature of Article 39 LED, these incongruences could result in further confusion and affect the ability of competent authorities to exchange vital information in emergencies.**

Lastly, note must be made of the apparent lack of a consistent approach in EU legal instruments regarding transfers of police and criminal justice data to non-competent recipients.[512] While the LED allows for and regulates such exchanges of personal data, this approach is not necessarily shared by all EU legislation in the area of freedom, security and justice. On the one hand, instruments such as the EPPO Regulation[513] and the Europol Regulation[514] contain a similar clause that authorises these institutions to transfer data to private recipients in third countries when warranted by exceptional circumstances. On the other, legislation such as the Eurojust Regulation[515] contains no such stipulation. While it naturally is beyond the LED to harmonise these instruments and this divergent approach might well be warranted, these disparities result in legal inconsistencies for the interaction between such European institutions and private entities or non-police bodies outside of the EU (see also section 2.5 on the fragmented data protection landscape within the AFSJ). Furthermore, similar issues might affect

[508] Marquenie, T., 'Article 39: Transfers of personal data to recipients established in third countries' in Kosta, E. and Boehm, F. (eds), *The Law Enforcement Directive: A Commentary*, Oxford University Press 2022 (forthcoming – under review).

[509] Winter, H.B. et al., *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, 2020.

[510] Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018).

[511] Wet van 5 augustus 1992 op het politieambt (Wet Politieambt) (B.S. 22 december 1992).

[512] Marquenie, T., 'Article 39: Transfers of personal data to recipients established in third countries' in Kosta, E. and Boehm, F. (eds), *The Law Enforcement Directive: A Commentary*, Oxford University Press 2022 (forthcoming – under review).

[513] Art. 84 EPPO Regulation mirrors Article 39 in full and comprises a nearly identical policy on these transfers. For more, see: Herrnfeld, H.H, 'Article 84 - Transfers of operational personal data to recipients established in third countries', in Herrnfeld, H.H., Brodowski, D. and Burchard, C., European Public Prosecutor's Office - Article-by-Article Commentary, Beck, Nomos & Hart, 2021.

[514] Art. 25(6) of Europol Regulation and its recently proposed amendments present a distinct but functionally similar approach to transfers to non-competent recipients in third countries. See: 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 ('Europol Regulation') (OJ L 135, 24.5.2016, p. 53).

[515] Section IV Eurojust Regulation does not provide in the possibility of transferring personal data to non-competent entities outside of the EU. See: 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 (OJ L 295, 21.11.2018, p. 138–183).

third country transfers in general. Shared European databases such as those instated by the SIS II[516] and Eurodac[517] regulations explicitly prohibit the transmission of their contents to recipients outside of the EU. This could complicate the operations of national competent authorities that might find themselves unable to transfer all necessary information if certain details were obtained from such a database. While this does not necessarily warrant a revision of the relevant instruments, **a further examination of these disparities in European legislation concerning the third country transfers of law enforcement data and information stored in adjacent European databases might be in order.**

[516] Art. 39 Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4–23). .

[517] Art. 35 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1–30).

7. INDEPENDENT SUPERVISORY AUTHORITIES

KEY FINDINGS

Concerns have been raised regarding the extent of the functional and practical independence of supervisory authorities in the context of law enforcement. While the structure of these authorities and the envisaged procedural safeguards can mitigate these potential issues, certain national implementations might be more prone to seeing a lessened degree of neutrality. It is of critical importance that supervisory authorities operate in an entirely independent manner and are provided with the resources to exercise their mandate and enforce the data protection standards imposed by the LED.

In comparison to the GDPR, the notably lower standards for the determination of the competence, tasks and powers of supervisory authorities under the LED are a point of contention. While national legislation implementing Articles 46 and 47 LED frequently expands upon the Directive's minimum standards, it remains regrettable that supervisory authorities are granted less extensive powers, especially in light of CJEU case law and the recommendations of data protection bodies. In addition, the exemption of courts and, optionally, independent judicial authorities acting in their judicial capacity risks undermining robust oversight of processing operations as few Member States appear to have introduced an effective alternative. Lastly, criticisms have been raised regarding the potential lack of engagement and cooperation between supervisory authorities in different countries as well as their participation in the EDPB.

With regards to prior consultation of the supervisory authority pursuant to Article 28 LED, questions have been raised regarding its alignment with recent EU case law on prior review of data access by law enforcement, as well as on the apparent discrepancies in the national interpretation and implementation of several aspects of this provision. Caution is due to ensure that the practical utility of this procedure is not undermined.

In order to provide for a high level of data protection and proper adherence to the rules established by the LED, Chapter VI introduces the independent supervisory authorities as a key measure to monitor and enforce legal compliance. The vital function exercised by these institutions is widely considered to be a critical aspect of the right to data protection[518] and indispensable for the safeguarding of the interests and freedoms of data subjects.[519] To ensure that the supervisory authorities can serve this role in an effective manner, the LED has laid out rules for their establishment, membership, independence, competence and powers. In the following section, particular attention is paid to a number of noteworthy aspects of their functioning and regulation.

7.1 Independence

For the supervisory authorities to be able to perform their tasks effectively, it is of vital importance that they operate in an independent manner. This principle was given shape through CJEU case law, as various judgments stressed the importance of keeping supervisory authorities free from external

[518] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology*, Vol. 33, No 3, 2019, pp. 249–270.

[519] Judgment of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650, para. 40.

influence. In Commission v. Germany, the Court established the criterion of 'complete independence' and noted that this applies to both direct and indirect forms of influence being exerted.[520] In the subsequent Commission v. Austria case, the Court determined that 'functional independence' alone was insufficient to guarantee the absence of outside influence and found that the Austrian data protection authority could not be considered entirely independent as its managing member was also a federal official holding a hierarchically superior position.[521]

Acknowledging this jurisprudence, Recital 75 LED reiterates that the independence of supervisory authorities is an essential component of data protection and Article 42 lays out further rules for its implementation. Among others, the provision necessitates that they must be free from all external influence and neither seek nor take instructions from outside sources. They must also be provided with sufficient resources to effectively perform their tasks and are free to choose their own staff. Furthermore, its members shall not engage in incompatible occupations and must be provided with sufficient resources to effectively perform their tasks, and any financial control that the organizations are under must not affect their independent nature. When examining the transposition of these provisions, it appears that these requirements have been fully incorporated into the national legal frameworks. In its recent report on the application and functioning of the LED, the European Commission noted that all Member States have stipulated the condition of independence in their transposing legislation.[522]

In practice, however, achieving complete and true independence could prove especially difficult in the context of law enforcement, as the oversight of police functioning is often exercised by different bodies within the same organisation.[523] Due to the particular nature of public security and criminal justice, it could be challenging for supervisory authorities to establish the necessary expertise and familiarity with police operations if they are unable to work closely with or recruit from organisations within this sphere. This issue might be more prominent in countries that have opted to establish a separate supervisory authority for the application of the LED. Pursuant to Article 41(3) LED, Member States have the possibility of instating a single authority to supervise both the LED and GDPR but are under no obligation to do so. While most Member States appear to have taken this joint approach[524], the countries of Sweden and Belgium have opted to assign these responsibilities at least in part to a separate body.[525] As noted by survey research[526], such a solution could result in a higher degree of expertise and knowledge of the specificities of police data processing, but it also risks diminishing the neutrality of the supervisory authority as the relevant experience was likely gained by previously being part of the police organisation. As a result, diligence should be exercised to avoid

[520] Judgment of 9 March 2019, *European Commission v. Germany*, Case C–518/07, ECLI:EU:C:2010:125, para. 30.

[521] Judgment of 16 October 2012, *European Commission v. Austria,* Case C-614/10, ECLI:EU:C:2012:631, paras. 42 and 50.

[522] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 11.

[523] Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', *Global Privacy Law Review*, Vol 1, No. 2, 2020, 102.

[524] This approach was also recommended by WP29. See: Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, 30.

[525] In Belgium, the role of the independent supervisory authority for law enforcement has been assigned to the Controleorgaan op de Politionele Informatie (COC, https://www.controleorgaan.be/). In Sweden, the supervisory authority competent for the GDPR, known as the Swedish Authority for Privacy Protection (IMY, https://www.imy.se/en/), shares the responsibility of monitoring law enforcement processing activities with another authority known as the Swedish Commission on Security and Integrity Protection (SINT, www.sakint.se).

[526] Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, 2020, 45.

undue external relationships or influence when it concerns the functioning and membership of supervisory authorities for law enforcement, regardless of whether the authority exists separately from the supervisory body under the GDPR.

An additional cause for concern regarding the independence of supervisory authorities in the context of law enforcement relates to the availability of resources. As noted above, it does not suffice for these authorities to be independent in standing and composition alone, but they must also possess the necessary resources, infrastructure, manpower and finances to duly exercise their tasks. In this light, the European Commission's recent report concluded that LED-related responsibilities are often not a priority among national supervisory authorities and that a majority of them have indicated that they lack sufficient resources and expertise to perform their duties.[527]

7.2 Competence, tasks and powers

Articles 45 through 47 of the LED lay out the tasks, competence and powers of the supervisory authorities. While these provisions intend to empower the authorities with robust capabilities to effectively monitor and enforce the relevant data protection standards, they nevertheless appear hampered by severe limitations and what scholars have described as a 'problematic lack of consistency' between the EU data protection instruments.[528]

First, mention must be made of the differences between the GDPR and LED in regard to the allocation of powers and tasks. Concerning their tasks, it is clear that the supervisory authority has fewer responsibilities under the LED than it does pursuant to the GDPR.[529] While most of the missing tasks are justifiable due to them corresponding to provisions with no bearing on police operations, the LED omits the assignments of listing requirements for DPIAs and fulfilling 'any other' tasks related to the protection of personal data. Nevertheless, the Directive somewhat compensates for this by establishing certain unique tasks of its own. For example, article 46(1)(g) LED introduces an additional assignment not found in the GPDR that requires the supervisory authority to review the lawfulness of data processing activities on behalf and on request of data subjects. Accordingly, legal scholars have noted that even though the supervisory authority's position is likely weaker under the LED than under the GDPR, it is still 'pretty strong' by nature.[530]

More serious discrepancies exist with regard to the supervisory authority's actual powers. As noted by legal scholars, the LED establishes a base set of powers that is significantly more limited in comparison to the GDPR without a clear justification for this deviation.[531] This is immediately clear from the wording used by the instruments themselves. While Article 83 GDPR asserts that supervisory authorities 'shall have all of the following (…) powers', Article 47 LED merely states that

---

[527] According to the report, a total of 16 supervisory authorities deemed their resources to be insufficient, and several of them indicated that this had negatively impacted their investigative activities, handling of complaints or issuing of opinions. For more, see: European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 21.

[528] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology,* Vol. 33, No 3, 2019, 13.

[529] Compare Art. 46 LED with Art. 57 GDPR.

[530] Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', *Global Privacy Law Review*, Vol 1, No. 2, 2020, pp. 93–103.

[531] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology,* Vol. 33, No 3, 2019.

these powers must be 'effective' and lists certain examples of what they might be, thus leaving it up to the discretion of the Member States to decide whether more extensive powers might be granted to the national supervisory authorities.

In contrast with the GDPR, the Directive significantly restricts the corrective powers of the supervisory authority by omitting the power to order compliance with data subject's requests and impose administrative fines. The latter, in particular, has been described as resulting in a 'relative weakness' of the LED's supervisory authorities when compared to the GDPR.[532] Furthermore, the LED does not provide the authority with the power to command the suspension of data flows to third countries. This results in the surprising lack of a clear power regarding the oversight of international transfers, especially when considering that case law like Schrems emphasized the importance of supervisory authorities in verifying the legal compliance of data transfers.[533] The same divergence can be observed with regard to the authority's investigative powers as well. Under the LED, it lacks the power to carry out investigations in the form of data protection audits, and to access law enforcement premises and processing equipment while gathering the information necessary for its tasks.

These disparities between both legal instruments have drawn criticism from data protection experts. The EDPS, for instance, argued that 'there is no need to differentiate between the powers conferred on Data Protection Authorities' under the GDPR and LED. In noting that supervision is a vital aspect of the right to data protection, it asserted that the level and intensity of supervision should not depend on the sector in which the processing takes place.[534] This opinion was shared by the former WP29 (now EDPB).[535] Some scholars have similarly posited that data processing in the context of law enforcement is 'arguably more important than in other branches of government', thus necessitating strong supervision and full protection as there is 'no apparent reason' to limit the LED's supervisory authority in this fashion.[536]

In practice, however, it appears that several Member States have expanded upon the minimum requirements established by the LED and, in this case, have further empowered their supervisory authorities in the context of law enforcement and criminal justice. For instance, the Irish Data Protection Act grants the supervisory Commission extensive corrective powers that more closely resemble the stipulations under the GDPR.[537] In addition to the LED's conditions, Article 127 allows the authority to issue reprimands, order compliance with data subject requests, command the communication of personal data breaches to data subjects, and order the suspension of international transfers. Similarly, Article 244§1 of the Belgian Data Protection Act awards the supervisory authority

[532] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology,* Vol. 33, No 3, 2019, 15.

[533] As noted by Drechsler, DPA's supervision powers over data transfers as part of their general obligations 'should also apply in the context of law enforcement.' This is in line with the opinion presented by WP29. See: Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, 30; Drechsler L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', *Global Privacy Law Review*, Vol 1, No. 2, 2020, 102.

[534] European Data Protection Supervisor, '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', 28 October 2015, 8.

[535] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, 30.

[536] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology,* Vol. 33, No 3, 2019, 11.

[537] Data Protection Act 2018 (Act 7 of 2018) (Iris Oifigiúl 42 p. 00752, 24 May 2018).

the competence to gain unlimited access to law enforcement premises, equipment and databases when necessary to obtain data required by their tasks, which is a power that was left out of the LED in comparison to the GDPR.[538] Furthermore, some countries also allow for more extensive sanctions. In Romania, for example, the supervisory authority has the ability to penalise competent authorities and impose fines up to 200.000 LEI, or around €40.000, for non-compliance with the transposed provisions of the LED.[539] As such, it seems that the Member States have made welcome additions to the powers of supervisory authorities and have addressed several of the abovementioned concerns regarding gaps in the LED. These findings are also corroborated by the European Commission's recent report on the Directive.[540] In its assessment, the Commission notes that "a majority" of Member States have been provided with other corrective and investigative powers. With regards to the former, it notes that "almost all" Member States have provided for the corrective powers as noted in the LED, while 18 Member States have chosen to equip their supervisory authorities with the capability to issue administrative fines, and that three of those have allowed them to impose these fines on natural persons or private entities as well. Regarding their investigative powers, the report establishes that a majority of national supervisory authorities have been granted additional capabilities to conduct audits, seize objects, copy data, or enter law enforcement premises as part of their investigation, thereby leading to the conclusion that "almost all data protection supervisory found that they have effective investigative powers".

This outcome, however, might still be less desirable than a consistent standard at the European level. Even though a majority of Member States have opted to expand the powers of their supervisory authorities, such an approach nevertheless risks an inconsistent set of powers across the EU, and still leaves a notable number of Member States that have chosen not to supplement the base requirements of the LED with additional capabilities. This lack of consistency could result in legal uncertainty and a fragmented framework consisting of countries with different levels and standards of supervisory oversight.

Second, the LED contains a significant exemption to the competence of the supervisory authorities. Pursuant to Article 45(2) LED, Member States are to exclude the processing operations of courts when acting in their judicial capacity from the supervisory authorities' scope of competence.[541] Per the European Commission's report, this restriction has been duly observed in all Member States.[542] Similarly, they have the discretion to apply the same restriction to other independent judicial

[538] Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018).

[539] The National Supervisory Authority for Personal Data Processing, 'Guidelines on the Application of Law No. 363/2018', 15, https://www.dataprotection.ro/servlet/ViewDocument?id=2127

[540] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 11-12.

[541] The same limitation of competence against courts in their judicial capacity is foreseen in the GDPR, under Article 55(3) of the Regulation. In this context, recent case law has established that the notion of acting in judicial capacity is to be interpreted broadly. In Case C-245/20, the CJEU held that the processing of personal data by courts in the context of their communication policy by, in this instance, making certain documents available to journalists, is considered an exercise of their judicial capacity and thus falls outside the jurisdiction of the supervisory authorities. While this judgment was issued in relation to the GDPR, it stands to reason that this interpretation applies to the LED in an identical fashion. For more, see: Judgment of 24 March 2022, X and Z v. Autoriteit Persoonsgegevens, C-245/20, ECLI:EU:C:2022:216.

[542] For additional information on the implementation of other competences of the supervisory authorities, in particular those relating to their involvement in judicial remedies and infringement procedures, reference can be made to the European Commission's report on the LED; European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 11-12.

authorities acting in the same capacity. Recital 80 provides further insight into the reasoning behind the former stipulation and clarifies that it exists to safeguard the independence of judges. Regarding the aforementioned other independent judicial authorities, the Recital notes that this could apply to bodies like the public prosecutor's office.

This restriction on the competence of supervisory authorities has garnered significant scholarly attention and has led to various concerns being raised.[543] As noted by the EDPS, the meaning and scope of various key concepts could remain subject to national differences and thus introduce divergent and ambiguous interpretations.[544] For example, what constitutes an 'independent judicial authority' and which actions are considered to be 'in judicial capacity' is likely to remain a matter of national interpretation.[545] Some data protection experts speculate that this may give rise to conflicts between data protection authorities and the judiciary as to ascertain whether the former is competent to monitor and review processing operations by judicial authorities.[546]

The final assurance presented in Recital 80 is similarly vague. In acknowledging the need of oversight of judicial authorities of any kind, the Recital notes that compliance with the rules of the Directive by courts and other independent judicial authorities nevertheless remains subject to independent supervision pursuant to Article 8(3) of the Charter.[547] Such a general approach, however, raises questions of its own. As evidenced by the CEG meetings[548], disagreements were raised as to whether a separate judicial body within the judiciary should be responsible for this task, or if this is already sufficiently ensured through normal procedures of judicial review and appeal.

While this exemption is justifiable, its scope and application can nevertheless be problematic.[549] **If individual Member States adopt significantly different interpretations of these concepts and place varying limits on the competences of supervisory authorities, the data protection landscape risks an extensive degree of fragmentation with regards to independent oversight**. In legal scholarship, such an outcome has been described as a 'harmonisation nightmare' that could 'undermine the whole Directive' as Member States move further apart in how they manage the supervision of data protection in the judiciary.[550] Such concerns appear valid, as relevant literature has demonstrated that Member States typically employ either an institutional or functional interpretation

---

543 Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology,* Vol. 33, No 3, 2019, pp. 249–70.

544 European Data Protection Supervisor, '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', 28 October 2015.

545 For an extensive review of the different interpretations of these concepts, see: Custers, B. et al., 'Quis custodiet ipsos custodes? Data protection in the judiciary in EU and EEA Member States', *International Data Privacy Law*, Vol. 12, Issue 2, 2022.

546 Di Francesco Maesa, C., 'Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)', *Eurojus Italia*, 24 May 2016, http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/.

547 Article 8(3) EU Charter notes that 'compliance with these rules shall be subject to control by an independent authority'.

548 Commission Expert Group, Minutes of the fifth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 18 January 2017.

549 Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology,* Vol. 33, No 3, 2019, 11.

550 De Hert, P. and Papakonstantinou, V., 'The New Police and Criminal Justice Data Protection Directive: A First Analysis', *New Journal of European Criminal Law*, Vol. 7, no. 1, 2016, 13.

of what constitutes a judicial authority acting in its judicial capacity, and that either approach leaves considerable room for divergent applications of these concepts under the LED.[551]

This issue could also be further exacerbated by both Article 1(3) LED, in explicitly stating that the Directive does not preclude Member States from providing higher data protection standards[552], and Article 45(2) LED, in noting that Member States remain free to expand this exemption to other independent judicial authorities.[553] Tensions might thus arise as some countries could seek to stretch the limits of the supervisory authority's competences over the judiciary while others could seek to exempt an increasingly large number of judicial authorities from its oversight altogether.[554]

In this context, mention deserves to be made of some national approaches to this issue.[555] As described above, Belgium, for instance, has taken the uncommon route of establishing a separate supervisory authority for the processing of personal data by police actors. Pursuant to its data protection legislation, this authority's competence is limited to the Belgian police agencies, the general oversight agency of law enforcement, the Passenger Information Unit, and, under certain conditions, the taxation administration.[556] Accordingly, it does not appear to exert competence over any judicial authorities and thus takes a notably restrictive approach to the scope of the supervisory authority's competence. A different perspective is present in the Irish Data Protection Act.[557] Rather than specify exactly which institutions the supervisory authority has competence over, Article 101(2) instead excludes data processing operations of the courts when acting in their judicial capacity. Of particular interest, however, is that the Irish law contains an additional and unique provision noting that the Chief Justice is to assign a particular judge to be responsible for the supervision of these operations. In particular, Article 157 notes that this judge shall handle complaints, promote awareness among judges of data protection standards, and ensure compliance with the provisions of the rules of the GDPR, LED and national law. In its subsequent articles, the Irish Act lays out specific rules and obligations for the processing of personal data by the judiciary. In doing so, it is one of the few countries to adopt specific data protection rules relating to the supervision of courts acting in their judicial capacity. Lastly, the Dutch legislation on the processing of judicial data carves out a notable role for its supervisory authority when it concerns judicial activities.[558] While Article 51h(7) of its Act on the processing of judicial data similarly excludes the operations of courts acting in their judicial capacity from the authority's supervisory competences, it nevertheless establishes rules for the oversight of judicial data

[551] For a more comprehensive overview of national perspectives, see: Custers, B. et al., 'Quis custodiet ipsos custodes? Data protection in the judiciary in EU and EEA Member States', International Data Privacy Law, Vol. 12, Issue 2, 2022.

[552] Di Francesco Maesa, C., 'Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)', *Eurojus Italia*, 24 May 2016, http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/.

[553] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

[554] An adjacent remark ought to be made regarding a notable error in the translation of this provision. In the English version of the text, Article 45(2) explicitly states that Member States shall provide for supervisory authorities not to be competent for the supervision of courts when acting in their judicial capacity. Yet the formal Dutch translation as published in the Official Journal of the European Union neglects to include the critical adverb 'not' and thereby results in a text that directly contradicts the intent behind this Article. In practice, however, this error appears to have been of no consequence as both the Dutch and Belgian laws adhere to the intended interpretation of Article 45.

[555] Custers, B. et al., 'Quis custodiet ipsos custodes? Data protection in the judiciary in EU and EEA Member States', International Data Privacy Law, Vol. 12, Issue 2, 2022.

[556] Art. 71 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018).

[557] Data Protection Act 2018 (Act 7 of 2018) (Iris Oifigiúl 42 p. 00752, 24 May 2018).

[558] Wet van 7 september 2000 houdende Justitiële en Strafvorderlijke gegevens (Wet Justitiële Gegevens, Stb. 2004, 129).

relating to criminal offenses. In absence of further exemption, this suggests that both the courts, when not acting in their judicial capacity, as well as other independent judicial authorities are subject to supervision by the data protection authority.

This brief comparison thus illustrates some of the abovementioned concerns. Certain countries, like Belgium, appear to significantly limit the scope of the supervisory authority's competence by applying it exclusively to police processing and excluding the processing of personal data by judicial authorities altogether, hereby leaving the oversight of their compliance with data protection law to the general court system. Yet others, such as Ireland and the Netherlands, exclude only the processing by courts in their judicial capacity from the scope of the supervisory authority's competence and thus might leave in place a significant degree of data protection-oriented oversight when it concerns various aspects of the judiciary, either by directly allocating some of these responsibilities to a particular judge or adopting additional rules on the supervisory authority's competence over the processing of judicial data. **While the LED identifies no specific approach as the most desirable or correct, these divergences could underlie future legal uncertainties, result in inconsistent applications of data protection standards, and hamper the cooperation between supervisory authorities in different countries**. Given that there appears to exist a potential gap in supervision, it is thus recommended that alternative steps are explored to implement some degree of oversight of further data processing operations in the context criminal justice and establish clear rules thereon. Such mechanisms have included the involvement of ombudspersons, higher courts, data protection officers, and dedicated committees or departments.[559]

Furthermore, a brief remark is due on the stipulations regarding international cooperation between supervisory authorities. While the LED contains a nearly identical provision on mutual assistance between these oversight bodies[560], it makes no mention of further methods of cooperation as identified by the GDPR. [561] These include joint operations, provisional measures by means of an urgency procedure, and the so-called consistency mechanism. Several of these omissions can be explained by the unique nature of law enforcement processing and the hesitancy surrounding the implication that police authorities might become subject to the scrutiny of a supervisory body of a different Member State[562], but the lack of some of these procedures, such as the consistency mechanism in particular, have been drawn into question.[563] This further ties into the role ascribed to the EDPB under the LED. While the EDPB is intended to play a vital part in ensuring consistency between different supervisory authorities under the GDPR, it fills no such role under the LED.[564] This stems, at least in part, from the fact that the supervisory authority for police does not necessarily hold a membership position at the

[559] Custers, B. et al., 'Quis custodiet ipsos custodes? Data protection in the judiciary in EU and EEA Member States', International Data Privacy Law, Vol. 12, Issue 2, 2022.

[560] See Art. 50 LED and Art. 61 GDPR.

[561] While likely not entirely related to these omissions, it is worth noting that the European Commission's recent report on the LED determined that the mechanism of mutual assistance between data protection authorities has been "very rarely utilized to date" . For more details on the practical application of this procedure, see: European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 25.

[562] Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.

[563] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology*, Vol. 33, No 3, 2019, 13.

[564] De Hert, P. and Papakonstantinou, V., 'The New Police and Criminal Justice Data Protection Directive: A First Analysis', *New Journal of European Criminal Law*, Vol. 7, No. 1, 2016.

EDPB.[565] Given that a recurring concern raised in this study relates to the lack of specific guidance applicable to the LED, it would be welcome if the supervisory authorities, or the respective departments therein, that focus primarily on police processing play a more prominent role in the EDPB.[566] **Accordingly, it is recommended that further steps are taken to ensure broader participation in or contributions to the EDPB by supervisory authorities under the LED.**[567]

7.3 Prior Consultation

While many of the supervisory authorities' responsibilities concern the processing of data by competent authorities or the exercise of data subject rights either after or during the processing operations, the LED has identified certain circumstances under which their involvement is due prior to the processing taking place. Pursuant to Article 28 LED, Member States shall provide for data controllers or processors to consult the supervisory authority prior to the processing activity in two cases. First, when the abovementioned data protection impact assessment indicates that the processing would result in a high risk in the absence of mitigation measures taken by the controller. As per 28(4), the data controller is required to provide the supervisory authority with the DPIA, thus making the authority aware of any plans to engage in high risk processing operations and establishing an avenue for prior consultation. Second, when the type of processing, in particular when using new technologies, mechanisms or procedures, involves a high risks to the rights and freedoms of data subjects.[568] This requirement therefore serves to engage the supervisory for any type of processing that poses a high risk to the rights of individuals regardless of whether a formal impact assessment indicates it as such in absence of further measures taken. Furthermore, the supervisory authority may establish a list of the processing operations subject to such prior consultation, and shall always be consulted during the preparation of proposals of legislative measures relating to data processing. In the event that the supervisory authority is consulted by the controller, Article 47(3) asserts that it must have effective advisory powers to advise the controller and, pursuant to Article 28(5), use any of its powers to if it opines that the intended processing would infringe upon the provisions of the LED, in particular where the controller has insufficiently addressed or mitigated the risks at hand. In this context, two remarks must be made.

The first concerns the scope of Article 28 itself and the manner in which it corresponds to CJEU case law. In the Digital Rights Ireland case, the Court ruled that law enforcement access to data retained by private actors must be dependent on a prior review by a court or independent administrative body.[569]

---

[565] Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology*, Vol. 33, No 3, 2019, 13.

[566] Similarly, the LIBE Committee recommended that the Commission examine whether there exist discrepancies in the guidance and recommendations issued by the EDPB with regards to the GDPR and LED. See: Chairman of Committee on Civil Liberties, Justice and Home Affairs, 'LIBE Contribution to the Commission upcoming report on the evaluation and review of the Law Enforcement Directive', IPOL-COM-LIBE D (2022)3535, 7 February 2022.

[567] Given that the EDPB's work programme for 2021-2022 indicates that the Board aims to focus on "encouraging and facilitating the use of the full range of cooperation tools enshrined in Chapter VII of the GDPR and Chapter VII of the LED", further guidance thereon can likely be expected in the near future. For more, see: European Data Protection Board, EDPB Work Programme 2021/2022, https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf.

[568] In this context, a parallel can be drawn with certain provisions of the proposed AI Act. At present, the draft version of this Regulation would require the provider of AI systems to conduct a conformity assessment that, in some instances, requires the involvement of a third-party notified body to verify conformity with the Act's standards. In the case of certain high-risk AI systems that are to be used in the context of law enforcement, it would fall upon the designated market surveillance authority to be notified and involved in the process of assessing the workings of the system. For more, see Chapter 4 and 5 of the Proposed AI Act.

[569] Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, C-293/12 and C-594/12, EU:C:2014:238, para. 62.

This condition was later reaffirmed in the Tele2 Sverige case.[570] Consequently, legal scholarship has raised the question whether the procedural safeguards established in the LED might satisfy the requirement ofprior review as established in CJEU case law.[571] At present, this is highly unlikely to be the case given two primary considerations. One, that law enforcement access to and further processing of personal data held by private entities would not necessarily constitute a high risk when performed in the context of criminal investigations rather than broader surveillance.[572] As a result, the scope of prior consultation under the LED is intentionally limited to processing activities that carry a particular risk rather than all those that involve the access to privately held data. Two, that the process of 'consultation' under the LED is not equivalent to the notion of 'review' as maintained by the CJEU. While Article 28(5) LED notes that the supervisory authority may use 'any of its powers referred to in Article 47', the clause concerning prior consultation (paragraph 3) only makes mention of an advisory role in this process, thus lacking an actual decision being issued or authorisation being granted. **Given that is not guaranteed that all national supervisory authorities would interpret these provisions in an identical manner, it is highly questionable and unlikely that these provisions establish a genuine process of review as intended by the CJEU and, according to some scholars[573], cannot be considered to serve as an implementation of the abovementioned rulings of the Court.** Naturally, it must be emphasized that the LED and data protection legislation in general were not envisioned as a solution to this issue in the first place. There are alternative approaches to be taken outside of data protection law, and requirements of prior review can similarly, and arguably better so, be achieved through criminal courts or other authorities in the justice system.

So while this remains noteworthy, it does not necessarily imply that Member States would fail to comply with the CJEU's jurisprudence by implementing the LED. The supervisory authorities under data protection law remain just one avenue of reviewing police operations and law enforcement processing of data. Other independent bodies or courts could still fill the same function, as appears to already be the case in certain European nations. In Lithuania, for example, it appears that national legislation on criminal procedure meets these requirements independently of data protection law.[574]

The second remark relates to possible inconsistencies in the national implementation of these provisions. In particular, the interpretation of Article 28(1) LED stating that it concerns processing that 'would result in a high risk *in the absence of* measures taken by the controller to mitigate the risk'. When considering the wording of this clause and the corresponding national provisions, it appears that two diverging approaches exist. On the one hand, a strict reading of this clause could signal that prior consultation is in order if the DPIA indicates that the processing would pose high risks in the hypothetical scenario where the controller neglects to implement mitigation measures. Or, put differently, that a high risk would exist if the processing operations were to continue as planned without mitigating measures being taken. Such a reading of the provision would thus require prior consultation whenever high risks are identified regardless of the impact of measures taken to mitigate them. At first sight, it appears that the Dutch version of the LED and, consequently, the Belgian and Dutch transposition thereof might be perceived as such. The translated text of these articles asserts

[570] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, para 120.

[571] Jasserand, C., 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?', *European Data Protection Law Review*, Vol. 4, No. 2, 2018, pp. 152–67.

[572] Ibid.

[573] Markevičius, E., 'Restrictions of Criminal Intelligence Measures in Law Enforcement Directive and Law on Criminal Intelligence of Lithuania', *Socrates*, Vol. 18, No. 3, 2020.

[574] Ibid.

that prior consultation is necessary when the processing would result in a high risk 'if the controller takes no measures to reduce the risk'.

On the other hand, this provision is more likely understood as meaning that prior consultation is only due if the residual risks remain high even after the adoption of such measures. This is the case in Article 84 of the Irish Data Protection Act that consolidates the provisions on the DPIA and prior consultation and, in doing so, it asserts that the controller shall consult the supervisory authority if it conducts an impact assessment and considers that the processing would result in a high risk to the rights and freedoms of individuals '*despite*' the implementation of safeguards. Accordingly, this provision suggests that no consultation would be necessary if a DPIA identifies high risks but the controller considers that the measures mitigate them sufficiently as to no longer be considered 'high'. Only if the risks remained high despite the adoption of such safeguards would prior consultation then be in order. This interpretation of it being the severity of the residual risks has been taken by certain data protection authorities[575], in regards to police processing, and WP29[576], with regard to the GDPR.

Considering the above and the purpose of Article 28, it stands to reason that the latter interpretation is correct. While the Recitals of the LED remain vague as to the scope of the prior consultation, Recital 84 GDPR explicitly notes that such involvement of the supervisory authority is warranted when the high risk identified by the DPIA cannot be mitigated by appropriate measures, in particular when this relates to the available technology and costs of implementation. **Regardless, the wording of this provision in the LED can be considered ambiguous, especially when examining its translation into certain languages. An appropriate level of caution is thus due**.

Finally, note must be made of an apparent omission in certain pieces of national legislation. As mentioned above, Article 28(1) LED refers to two situations in which prior consultation is necessary. While (a) hinges the involvement of the supervisory authority on the result of the DPIA, (b) simply asserts that such a consultation is also in order when the type of processing, in particular where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects. This clause thus suggests that prior consultation might be necessary even in the absence of a DPIA. In transposing this provision, however, not all Member States appear to have included this possibility. For instance, Article 84 of the Irish Data Protection Act makes no mention of this part of the LED and only requires prior consultation in the event that a DPIA yields certain results.[577] Such an approach thus appears to diverge from the broader safeguards provided in the LED, as high risk processing operations would not necessarily require the prior involvement of the independent supervisory body.

[575] Information Commissioner's Office (ICO), 'Guide to Law Enforcement Processing – Do we need to consult the ICO?', 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/do-we-need-to-consult-the-ico

[576] Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', WP248, 2017, https://ec.europa.eu/newsroom/article29/items/611236

[577] Data Protection Act 2018 (Act 7 of 2018) (Iris Oifigiúl 42 p. 00752, 24 May 2018).

8. EX POST EVALUATION OF THE LED BY THE EUROPEAN COMMISSION

KEY FINDINGS

It may be questioned to what extent the standard of high quantitative and qualitative data imposed by the Better Regulation Guidelines has been met by the sources used for the First Report on the LED application and functioning by the European Commission.

Looking ahead to the second report on the evaluation and review of the LED scheduled in 2026, a strong continuous monitoring and ex post evaluation system should provide for sufficient information on the effectiveness, efficiency, relevance, coherence, and EU added value of the LED transposed into national law. To that end, attention should be paid to the collection of wide range of data from a variety of sources, including the different LED competent authorities, the national data protection supervisory authorities, civil society organisations and citizen representations, as well as EU institutions and relevant EU agencies. The evaluation should be performed on the basis of the two primary objectives of the LED, that is the protection of citizens' fundamental rights and freedoms, particularly the right to the protection of personal data, and the unrestricted exchange of personal data by competent authorities within the EU.

According to the Better Regulation Guidelines, the European Commission should have in place a monitoring system in order to evaluate through an evidence-based approach the performance of an EU legislation.[578] In this way, sufficient information, that is qualitative and quantitative data, should be gathered by the European Commission in order for it to perform its task of monitoring and evaluating legislation such as the LED. As pointed out, 'high quality policy implementation relies on quantified impact assessments that draw on previous evaluations and are supported by evaluation and monitoring plans that, in turn, are supported by strong data collection processes'.[579]

For its First Report on the LED application and functioning, which was published with more than two months delay, the European Commission relied on contributions from EU institutions and national data protection supervisory authorities. Additional feedback was received from only 17 civil society organisations and 9 public responses to a public call for evidence.[580] The European Commission report further mentions that it is based on the information provided by Member States when notifying to the Commission the measures taken to transpose the LED, as well as it is supported by an external study carried out by an external contractor, about which no further information or reference is provided.[581] On the basis of its structure, the report relies to a large extent on the input collected by the EDPB from

[578] European Commission, Commission Staff Working Document Better Regulation Guidelines, SWD(2021) 305 final, 3 November 2021.

[579] Jones, S., Briefing requested by the IMCO Committee 'Identifying Optimal Policy Making and Legislation', European Parliament Policy Department for Economic, Scientific and Quality of Life Policies, PE 638.399, May 2019; S. Jones, G. Dohler and L. Plate Briefing requested by the JURI committee 'Better regulation in the EU: Improving quality and reducing delays', Policy Department for Citizens' Rights and Constitutional Affairs, PE 734.712, June 2022.

[580] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 7.

[581] Ibid, p. 8.

the national data protection supervisory authorities through questionnaires on their statistics and experience.[582] Finally, the European Commission admitted to having found it 'difficult to compile statistics on the application of the LED'.[583] It may therefore be questioned to what extent the standard of high quantitative and qualitative data has been met.

Given the drastic change in scope from the previous CFD framework that only regulated cross-border criminal justice processing of personal data, to the new LED full system of rights and obligations for all criminal justice data processing, as well as the short in time application of the LED due to delayed national transpositions, information on its effectiveness and coherence may indeed still be scattered or incomplete. However, looking ahead to the second report on the evaluation and review of the LED scheduled in 2026, pursuant to Article 62(1) LED, a strong continuous monitoring and ex post evaluation system should provide for sufficient information on the effectiveness, efficiency, relevance, coherence, and EU added value[584] of the LED transposed into national law. To that end, attention should be paid to the collection of wide range of data from a variety of sources on a continuous basis.[585] In LED terms, that includes the different entities that fall under the definition of competent authority under Article 3(7) LED, the national data protection supervisory authorities, civil society organisations and citizen representations, as well as EU institutions such as the EDPS and the EDPB and EU agencies that collaborate with competent authorities such as Europol. The evaluation should be performed on the basis of the two primary objectives of the LED, that is the protection of citizens' fundamental rights and freedoms, particularly the right to the protection of personal data, and the unrestricted exchange of personal data by competent authorities within the EU.

More specifically, precise data on national practices should include at least the following.[586] Competent authorities should provide input first on the exercise of data subject's rights: the number of requests per right and per Member State, including potential grounds for refusal and requests for human intervention under Article 11 LED. Second, information should be provided on the use of processors, including the use of private contractors, per Member State and activity. Third, data on the use of AI and other intrusive technologies such as for instance Pegasus should inform on the scope and legal basis for deployment, as well as the frequency at which new technologies, as referred to by Articles 28 and 29 LED, are implemented and used in practice. Fourth, information should be collected on cross-border and international data transfers, including data exchanges with EU institutions, per country and per legal basis used under Articles 36-39 LED. Fifth, the efforts towards promoting a data protection culture and awareness through national and cross-border trainings should be documented. In that regard, the establishment of the Network for the Data Protection Officers of competent authorities referred to in the European Commission report[587], is an important initiative that should facilitate the gathering of such information.

---

[582] Ibid, p. 16-34.

[583] Ibid, p. 8.

[584] European Commission, Commission Staff Working Document Better Regulation Guidelines, SWD(2021) 305 final, 3 November 2021.

[585] See also S. Jones, G. Dohler and L. Plate, Briefing requested by the JURI committee 'Better regulation in the EU: Improving quality and reducing delays', Policy Department for Citizens' Rights and Constitutional Affairs, PE 734.712, June 2022.

[586] See also Chairman of Committee on Civil Liberties, Justice and Home Affairs, 'LIBE Contribution to the Commission upcoming report on the evaluation and review of the Law Enforcement Directive', IPOL-COM-LIBE D (2022)3535, 7 February 2022.

[587] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 19.

Input from national supervisory authorities should continue to be collected, as thoroughly demonstrated in the EDPB contribution[588]. Data should continue to be provided on the number and content of complaints lodged, the number and results of indirect access requests submitted as well as on the use of their powers for enforcement of the LED, including details on their human, financial and technical resources, use of powers through oversight activities, as well as issuing enforcement and advisory decisions.

Finally, input from civil society organisations should concern their activity within and across Member States, including information on their representation of data subjects. The European Commission should ensure that the stakeholder consultation process takes duly into account minoritized and systematically under-represented organisations and communities, for example communities that have been victims to biased police practices including through the use of intrusive algorithmic tools.[589]

The collection of input may be further facilitated by the deployment of new technologies on behalf of the national authorities and European bodies.[590] For instance, several processes may be automated, including the logging of prior consultations requested and complaints lodged before supervisory authorities and resulting outcomes, the submission of questionnaires addressed to stakeholders, the comparison of data throughout periods of time, and so on. In this way, the evaluation of the LED implementation and enforcement can take place in a more holistic and continuous basis, properly identifying where its transposition is successful in pursuing the objectives it sets out to deliver, and where it produces side effects, unwanted outcomes or fails to produce the intended outcomes.[591]

[588] European Data Protection Board, Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, 14 December 2021.

[589] See also Renda, A. In-Depth Analysis requested by the JURI committee, 'Assessment of current initiatives of the European Commission on better regulation', Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 734.766, June 2022.

[590] See also Sartor, G., In-Depth Analysis requested by the JURI committee, 'The way forward for better regulation in the EU – better focus, synergies, data and technology', Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 736.129, August 2022.

[591] Ibid.

9. CONCLUSIONS: OPEN QUESTIONS AND RECOMMENDATIONS

9.1 Concluding remarks and open issues

The Law Enforcement Directive (LED) constitutes an ambitious and significant step forward for the protection of personal data in the context of policing and criminal justice. Building upon the foundations of Directive 95/46/EC, Framework Decision 2008/977/JHA, and the Council of Europe Recommendation R(87)15, the LED marks the first EU legal instrument to introduce data protection safeguards for domestic processing operations by law enforcement agencies and criminal justice authorities. In doing so, it established a robust framework of high standards and a strong emphasis on the protection and exercise of data subject rights. The LED largely mimics the structure of the GDPR and reflects many of the same rules regarding the adherence to general data protection principles, the empowerment of data subjects, the obligations placed on competent authorities, the transfers of personal data to third country recipients, and the independent supervision of legal compliance with these norms.

While the advancements made with the LED are laudable, its efficacy, reliability and potency are nevertheless hindered by various shortcomings. Opting for a Directive instead of a Regulation has allowed for a multitude of diverging approaches to data protection standards, thus resulting in a continued lack of harmonisation and legal uncertainty in the AFSJ. This is exacerbated further by key concepts remaining subject to national interpretation, thereby giving way to highly inconsistent applications of critical concepts like public security, criminal offense and competent authority. Moreover, the sectoral instruments such as the Europol Regulation could lead to a fragmented and asymmetrical application of data protection rules within the AFSJ.

Issues have also been observed resulting from the lack of certain general principles that are present in the GDPR, and the impact of ambiguous stipulations and inconsistently implemented provisions on the re-use, storage and categorisation of personal data. With regard to the exercise of data subject rights, concerns have been raised about the absence of certain responsibilities and the flawed transposition of several provisions regarding the exercise and restriction of certain rights, in particular when considering the broad discretion enjoyed by Member States in this context.

Furthermore, the concrete obligations placed upon data controllers are often lacking in comparison to their GDPR counterparts, are faced with disparate national implementations and practical difficulties, and suffer from the absence of concrete guidance provided to competent authorities. This is particularly notable within the provisions regarding joint controllership, data protection impact assessments and the logging of processing operations. As for transfers to third countries, the lack of adequacy decisions and the difficulties associated with uncoupling them from the workings of the GDPR risks undermining the protection of EU fundamental rights beyond the Union's borders. This is compounded by the continued reliance on pre-existing transfer agreements that are unlikely to meet current data protection standards, and by the risks associated with making local competent authorities responsible for resolving complicated issues of adequacy and equivalence without extensive guidance. Regarding independent supervision of legal compliance, the comparatively limited powers and tasks awarded to the supervisory authorities stand to decrease their effectiveness, while issues surround the procedure of prior consultation. As Member States seem to be given a wide discretion on the application of the LED to processing operations by courts and judicial authorities, there even exists a serious risk that such authorities might avoid potent oversight altogether.

Although these issues do not invalidate the important contributions that the LED has made to the European data protection framework, they risk undermining its potency and consistency to the

detriment of legal certainty and the rights and freedoms of EU data subjects. The limited attention and lack of guidance regarding the implementation of the LED on an EU level, for instance from the EDPB, further exacerbate the legal uncertainty and inconsistency. In light of the above, the following section thus presents several recommendations to address these limitations and strengthen the functioning of data protection law in the context of law enforcement and criminal justice.

9.2 Recommendations

Member States:

Member States are encouraged to further clarify and delineate several LED provisions in their implementing acts, as also pointed out by the European Commission's report. More specifically, the scope of the LED should be restricted to criminal offences and criminal justice matters; entities such as transportation authorities that are in charge of primarily administrative offences are likely better subject to the GDPR instead of the LED. The scope of application of the LED vis-à-vis courts and judicial authorities should be further clarified. It is further recommended that particular attention is paid to the interpretation of the data protection principles, in line with the Charter, EU case law and international data protection instruments. For instance, the mention to 'not excessive' within the data minimisation principle should be interpreted narrowly. Clear criteria for setting time frames In relation to storage limitation should be accompanied by procedural requirements (for example oversight, DPO). The inclusion of safeguards for minors and other vulnerable groups is encouraged.

Insofar as data subject's rights are concerned, it is encouraged to provide information under Article 13(2) proactively and in general, not only in specific cases. Timeframes for reacting to data subject's rights' request should be defined in national laws and not by individual controllers. The restriction of processing should be established within national laws as a standalone right. The effective indirect exercise of rights by the supervisory authority should be monitored and ensured. Article 17 should not function as an alternative to the direct exercise of rights nor be assimilated with the process of lodging a complaint before the supervisory authority.

Regarding the implementation of the data controller obligations under Chapter IV, Member States are advised to closely monitor the national transposition of the logging requirements for which the LED has allowed a longer period of implementation. It is important that the envisioned timeline to integrate technical logging measures is met by Member States and that further clarity is provided regarding the management, supervision, use and storage of logs. Similarly, it is advised that further attention is placed on providing a greater degree of consistency, transparency and clarity with regards to certain aspects of data protection policy, such as the arrangements made between joint controllers, in particular with regards to the establishment of a single point of a contact and the availability of information to data subjects.

Concerning the transfers of personal data to third country recipients, Member States are strongly encouraged to pay renewed attention to the alignment of pre-existing legal instruments for international transfers with modern data protection standards in the LED. At present, there remains a notable risk that various international agreements adopted prior to the LED contain insufficiently potent data protection standards and might thus undermine the protection of the rights of EU citizens in third countries.

With regards to the establishment and functioning of supervisory data protection authorities, Member States are encouraged to ensure that their full independence is assured both in terms of remaining free from external interference and having access to sufficient resources, expertise and manpower. In addition, it is advisable that the tasks and powers assigned to these authorities are expanded and

further aligned with the more extensive capabilities awarded thereto under the GDPR. While the monitoring of courts acting in their judicial capacity is explicitly excluded from their competences, it is nevertheless advised that alternative steps are considered to establish some mechanism for oversight in this context.

National competent authorities:

National competent authorities within the meaning of Article 3(7) LED are urged to observe the compliance with the data protection principles. In particular, competent authorities should ensure a significant degree of transparency. Although the levels of transparency of processing operations are to be adapted to the specific needs of each authority, it should be kept in mind in mind that not all LED subject processing activities are in need of protection from publicity, but on the contrary some must be made available to the public. The application of the purpose limitation principle could be further supported through impact assessment and technical and by design tools.

Insofar as data categorisation is concerned, the defined categories should not be static but adaptable, otherwise the practice defeats the purpose of these provisions. Different safeguards, including time limits, for different categories of data subjects may be encouraged, especially for vulnerable data subjects or non-suspects, insofar as it is practically possible. Should practice reveal that this provision cannot be practically be enforced, competent authorities may consider alternatives following the Europol system or other (pre-existing) systems developed by European bodies or national competent authorities.

Competent authorities should look for certified and/or auditable on national, international or European level AI systems to be deployed in order to facilitate their work. They should not opt for technologies that are subject to legal constraints, such as IP rights, excluding the provision of explanations on how a system works.

The restriction of data subject's rights should be subject to a narrow interpretation and application. The LED does not allow a blanket restriction of rights; in other words, data subjects should be informed of any processing activity relating to them as soon as the condition of restriction no longer applies, even without prior request, in line with the jurisprudentially established notification duty.

Any derogation from the LED data subject's rights where personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings should not result in lower standards of protection.

Additionally, the provision of information to be made available and the exercise of data subject's rights should be facilitated and streamlined. For example, single points of contact and/or dedicated websites including all required information as well as template for requests should be set up. Requirements for the exercise of a data subject's right, which are not clearly foreseen in national laws or even go against the spirit and wording of the LED, such as proof of residence within a specific Member State, should be abolished. Information on automated-decision making, albeit not explicitly required under Article 14, should be provided in line with Article 11 and Recital 38. Furthermore, competent authorities are encouraged to closely adhere to the standards under Chapter IV. Regarding the practice of logging data processing activities, competent authorities are advised to take a proactive rather approach to managing system logs by actively using them for self-audits and periodical assessments, and to ensure that the use of system logs is reserved solely for the intended purposes rather than general police operations. When conducting a Data Protection Impact Assessment, competent authorities are to not just consider the implications of high risk processing activities from a data protection perspective but to also examine their impact on human rights in general and, where necessary, involve the supervisory authority in this process.

National supervisory authorities:

With regards to the critical role that national supervisory authorities play in the monitoring of legal compliance and informing of competent authorities, a number of recommendations are to be made relating to the exercise of their tasks. In general, the national supervisory authorities that are competent for the enforcement of both the GDPR and LED are encouraged not to deprioritize the processing of personal data by law enforcement but to allocate sufficient manpower and resources to the application and monitoring of the LED. Additionally and insofar as the process of conducting a Data Protection Impact Assessment is concerned, the national supervisory authorities are strongly encouraged to provide more extensive guidance specifically tailored to the domain of law enforcement and taking into account its unique nature while aligning its standards with the increased level of detail provided by the GDPR. Furthermore, it is recommended that the extent of cooperation between supervisory authorities under the LED is expanded and that the divisions or bodies focused on police processing contribute further to the EDPB.

EU legislator and policy bodies, including European Commission, EDPS and EDPB:

The EU legislator and policy bodies have a crucial role to play in the implementation of the LED. Further guidance should be provided on its delineation with the GDPR as well as sector-specific data protection frameworks. First, the definition of 'criminal offence' which is autonomous under EU law should be further clarified in a more homogeneous and harmonious amongst Member States manner. By consequence, the authorities that should be covered by the LED, including those that are founded on the basis of EU law such as FIUs, should be delineated and streamlined. Second, the alignment of the LED with the AFSJ data protection framework should be clarified in a manner that upholds a hight level of protection. The application of the EUDPR Chapter IX throughout the AFSJ should be reconsidered, at least in relation to the main principles and obligations. Otherwise, it is encouraged to provide further guidance on the alignment and application of the different data protection frameworks applicable to the EU agencies and databases with which the national competent authorities collaborate. Any divergence from the core data protection framework, that is GDPR, LED and EUDPR, should be specifically justified, as well as strictly regulated and applied.

EU bodies should provide further guidance on several LED provisions that have been deemed as controversial, in order to ensure alignment with the Charter and Article 8 therein. For example, guidance is needed on Article 4(2) and the principle of purpose limitation, what 'subsequent processing' means and how to assess compatibility of law enforcement purposes, especially in light of potentially divergent national implementations given broad discretion. Further elaborate upon and specify the concepts of 'automated decision-making solely based on automated means, including profiling' as well as 'human intervention', for instance taking into account the different stages involved before a decision produces effects on the individual, and by establishing a requirement of reasoned scrutiny for human intervention to be meaningful. Similarly, EU bodies are encouraged to examine the level of detail provided by national data protection policy with regards to certain provisions and consider the desired degree of specificity in this context. For instance, the legal requirements for information and data security in law enforcement systems are often quite general and do not provide particular standards for the security of processing operations. Assessing whether such standards are laid out in internal or organizational policies and are in line with the envisioned level of security is thus advisable. Strong oversight and guidance is strongly encouraged with regards to the practicalities surrounding the exercise of data subject's rights and the applicable restrictions thereof.

Additional efforts from EU bodies are also encouraged regarding the transfers of personal data to third country recipients. In particular, a strong emphasis should be placed on adopting future adequacy

decisions pursuant to the LED in order to provide in a robust framework of adequacy decisions serving as a consistent, clear and legally sound basis for third country transfers. In doing so, a clear decoupling from the motivations underlying the GDPR should be maintained and particular attention should be paid to the unique nature of law enforcement. Regarding transfers under appropriate safeguards or exceptional transmissions to non-competent recipients, it is advised that EU bodies focus on improving legal certainty and providing further clarity on the requirements and considerations for such transmissions of personal data. In addition, it is recommended that further guidance and clarity is provided to support competent authorities in assessing critical concepts such as essential equivalence and appropriate safeguards, and that their responsibilities in assessing third country data protection standards and human rights guarantees are further examined and clarified. Consideration ought to be given to nationally divergent interpretations and, where possible and necessary, aligned as such.

Lastly, with regards to the national supervisory authorities, EU bodies are encouraged to ensure the consistent and proper implementation of all relevant provisions of the LED into national law in order to avoid potential deviations from the strong safeguards provided by the Directive with relation to the exercise and assignment of their tasks and duties. Similarly, EU bodies are advised to further emphasize and support cooperation between independent supervisory authorities under the LED and necessitating their involvement in or contribution to the EDPB.

Finally, the European Commission, in the context of its continuous monitoring and assessment of implementation of LED provisions, should strive to improve the quality and quantity of data required for the ex post evaluation of the implementation of the LED into national laws. A wide range of data should be collected from a variety of sources, including the different LED competent authorities, the national data protection supervisory authorities, civil society organisations and citizen representations, as well as EU institutions and relevant EU agencies. Particular attention should be paid to data protection principles, data subject's rights, legal grounds for data processing, including through automated decision making systems, data transfers and the use of national supervisory authorities' powers.

REFERENCES

Doctrine

- Alonso Blas, D., 'Ensuring Effective Data Protection in the Field of Police and Judicial Activities: Some Considerations to Achieve Security, Justice and Freedom', *ERA Forum,* Vol. 11, no. 2, 2010, pp. 233–50
- Bäcker, M. and Hornung, G., 'Data Processing by Police and Criminal Justice Authorities in Europe – The Influence of the Commission's Draft on the National Police Laws and Laws of Criminal Procedure', *Computer Law & Security Review*, Vol 28, No. 6, 2012, pp. 627–33.
- Bieker, F., Friedewald, M., Hansen, M., Obersteller, H. and Rost, M., 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' in *Privacy Technologies and Policy*, Cham, 2016, pp. 21–37.
- Binns, R. and Veale, M., 'Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR' *International Data Privacy Law*, Vol. 11, No. 4, 2021.
- Bolognini, L., A Proposal for the EU Privacy Law Simplification, Supporting Data-Driven Research in the Law Enforcement Field', Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP), 10 January 2020, available at https://www.istitutoitalianoprivacy.it/2020/01/10/a-proposal-for-the-eu-law-simplification-supporting-data-driven-research-in-the-law-enforcement-field/.
- Boulet, G. and De Hert, P., 'Cooperation between the private sector and law enforcement agencies: an area in between legal regulations', in Aden H. (ed.), *Police Cooperation in the European Union under the Treaty of Lisbon - Opportunities and Limitations*, Nomos Verlagsgesellschaft 2015.
- Brewczyńska, M., 'Financial Intelligence Units: Reflections on the Applicable Data Protection Legal Framework', *Computer Law & Security Review,* Vol. 43, 2021, pp. 105612.
- Brewczyńska, M., '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 Kosta and Leenes (eds) *Research Handbook on EU data protection* (Edward Elgar 2022).
- Broekhuijse I., Ballin E.H. and Ranchordás S., 'The Constitutions of the Dutch Caribbean: A Study of the Countries of Aruba, Curaçao and Sint Maarten and the Public Entities of Bonaire, Sint Eustatius and Saba' in Albert R., O'Brien D. and Wheatle S. (eds.), *The Oxford Handbook of Caribbean Constitutions*¸ Oxford University Press 2020.
- Brouwer, E., 'Private Life and Data Protection in the Area of Freedom, Security and Justice' in Iglesias Sánchez, S. and González Pascual, M. (eds), *Fundamental Rights in the EU Area of Freedom, Security and Justice*, Cambridge University Press, 2021.
- Brown, I. and Korff, D., 'Exchanges of Personal Data After the Schrems II Judgment', European Parliament Committee on Civil Liberties (LIBE), July 2021.
- Cannataci, J. A. and Caruana, M. M., 'Recommendation R (87) 15 – Twenty-Five Years down the Line', Council of Europe, Strasbourg, T-PD(2013)11, 18 February 2014.
- Caruana, M., 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement', *International Review of Law, Computers & Technology* Vol. 33, No 3, 2019, pp. 249–70.

- Castets-Renard, C., 'Human Rights and Algorithmic Impact Assessment for Predictive Policing' in Micklitz, H.W., Pollicino, O., Reichman, A., Simoncini, A., Sartor, G. and De Gregorio, G. (eds), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, 2021.
- Chambers and Partners, *Data Protection & Privacy 2021, Practice Guides,* Hungary, last updated 09 March 2021, available at: https://practiceguides.chambers.com/practice-guides/comparison/627/6267/10386-10395-10401-10406-10414.
- Cocq, C., 'EU Data Protection Rules Applying to Law Enforcement Activities: Towards an Harmonised Legal Framework?', New Journal of European Criminal Law, Vol. 7, No. 3, 2016, pp. 263–76.
- Colonna, L., 'The New EU Proposal To Regulate Data Protection in Law Enforcement Sector: Raises the Bar But Not High Enough', *IRI Promemoria*, Institutet för rättsinformatik, Juridiska fakulteten, Stockholms universitet, Stockholm, 2012.
- Coudert, F., Dumortier, J. and Verbruggen, F., 'Applying the Purpose Specification Principle in the Age of "Big Data": The Example of Integrated Video Surveillance Platforms in France', ICRI Research Paper 6, 2012, available at https://papers.ssrn.com/abstract=2046123.
- Custers, B. et al., 'Quis custodiet ipsos custodes? Data protection in the judiciary in EU and EEA Member States', *International Data Privacy Law*, Vol. 12, Issue 2, 2022.
- De Hert, P. and Papakonstantinou, V., 'The New Police and Criminal Justice Data Protection Directive: A First Analysis', *New Journal of European Criminal Law*, Vol. 7, No. 1, 2016, pp. 7–19.
- De Hert, P. and Sajfert, J., 'The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680', Brussels Privacy Hub Working Paper 7, no. 31, December 2021.
- Demetzou, K., 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation', *Computer Law & Security Review*, Vol. 35, 2019.
- Di Francesco Maesa, C., 'Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)', *Eurojus Italia*, 24 May 2016, http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/.
- Dimitrova, D., and De Hert, P., 'The Right of Access Under the Police Directive: Small Steps Forward' *Privacy Technologies and Policy*, Medina, M. et al, (eds), Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 111–30.
- Domingo Sanchez, M.B., 'The protection of personal data in the area of freedom, security and justice: special consideration of data transfers to third countries and international organizations according to directive 2016/680', *Revista de Estudios Europeos*, No. 69, 2017.
- Drechsler, L., 'Comparing LED and GDPR Adequacy: One Standard Two Systems', Global Privacy Law Review, Vol. 1, No. 2, 2020, pp. 93–103.
- Drechsler, L., 'The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive', *Cybercrime: New Threats,*

New Responses - Proceedings of the XVth International Conference on Internet, Law & Politics, Barcelona, 1-2 July, Huygens Editorial 2020.

- Drechsler, L., 'EDPB Issues Guidance on Personal Data Transfers Based on Adequacy Decisions in the Context of the Law Enforcement Directive', *European Data Protection Law Review*, Vol. 7, No. 2, 2021.
- Drechsler, L., 'Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context', *International Data Privacy Law*, Vol. 11, No. 2, 2021, pp. 182-195.
- Drechsler, L. and Kamara, I., 'Essential equivalence as a benchmark for international data transfers after Schrems II' in Kosta E. and Leenes R. (Eds.), *Research handbook on EU data protection*, Edward Elgar 2022.
- Ebers M. et al., 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)', J Vol. 4, No. 4, 2021, pp. 589–603
- Emanuilov, I., Fantin, S., Marquenie, T. and Vogiatzoglou, P., 'Purpose Limitation By Design as a Counter to Function Creep and System Insecurity in Police AI', *UNICRI Special Collection on AI*, 2020, pp. 26-37.
- Fantin, S., 'Law enforcement and personal data processing in Italy: implementation of the Police Directive and the new data retention law', CiTiP Blog, 29 May 2018, available at https://www.law.kuleuven.be/citip/blog/law-enforcement-and-personal-data-processing-in-italy-implementation-of-the-police-directive-and-the-new-data-retention-law/.
- González Fuster, G., 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights', European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 656.295, 2020.
- Herrnfeld, H.H, 'Article 84 - Transfers of operational personal data to recipients established in third countries', in Herrnfeld, H.H., Brodowski, D. and Burchard, C., *European Public Prosecutor's Office - Article-by-Article Commentary*, Beck, Nomos & Hart, 2021.
- Hudobnik, M., 'Data Protection and the Law Enforcement Directive: A Procrustean Bed across Europe?', *ERA Forum*, Vol. 21, No. 3, 2020, pp. 485–500.
- Jasserand, C., 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?', *European Data Protection Law Review*, Vol. 4, No. 2, 2018, pp. 152–67.
- Jasserand, C., 'Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?', *Computer Law & Security Review*, Vol. 34, No. 1, 2018, pp. 154–65.
- Jones, S. Dohler G. and Plate L., Briefing requested by the JURI committee 'Better regulation in the EU: Improving quality and reducing delays', Policy Department for Citizens' Rights and Constitutional Affairs, PE 734.712, June 2022.
- Jones, S., Briefing requested by the IMCO Committee 'Identifying Optimal Policy Making and Legislation', European Parliament Policy Department for Economic, Scientific and Quality of Life Policies, PE 638.399, May 2019.

- Koning, M. E., *The Purpose and Limitations of Purpose Limitation,* Radboud University Nijmegen, Utrecht, Netherlands, 2020.
- Kosta, E., 'A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon', *Research Handbook on EU data protection*, Kosta, E. and Leenes, R. (eds), Edward Elgar, 2022 (forthcoming).
- Leiser, M. and Custers, B., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, Vol. 5, No. 3, 2019, pp. 367–78.
- Lequesne Roth, C., Kimri, M., and Legros, P., 'La Reconnaissance Faciale dans l'espace public – Une cartographie européenne', [Rapport de recherche] Université Côte d'Azur, Nice, France, 2020, ffhal-03133123f.
- Lynskey, O., 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' *International Journal of Law in Context*, Vol. 15, No. 2, 2019, pp. 162–76.
- Markevičius, E., 'Restrictions of Criminal Intelligence Measures in Law Enforcement Directive and Law on Criminal Intelligence of Lithuania', *Socrates*, Vol. 18, No. 3, 2020.
- Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340.
- Marquenie, T., 'Legal and Ethical Challenges in Algorithmic Policing and Law Enforcement AI' in Bourguignon, M., Hick, T., Royer, S., Yperman, W. (eds), *Technology and Society: The Evolution of the Legal Landscape*, Gompel & Svacina, 2020.
- Marquenie, T., 'Article 39: Transfers of personal data to recipients established in third countries' in Kosta, E. and Boehm, F. (eds), *The Law Enforcement Directive: A Commentary*, Oxford University Press 2022 (forthcoming – under review).
- Marquenie, T. and Quezada-Tavárez, K., 'Data Protection Impact Assessments in Law Enforcement: Identifying and Mitigating Risks in Algorithmic Policing' in Markarian, G., Nitsch, H., Karlovic, R. and Chandramouli, K. (eds), *Security technologies and social implications: An European Perspective*, Wiley-IEEE Press, 2022 (under review).
- Marquenie, T. and Quezada-Tavárez, K., 'Operationalization of Information Security through Compliance with Directive 2016/680 in Law Enforcement Technology and Practice' in Vedder, A., Schroers, J., Ducuing, C. and Valcke, P. (eds), *Security and Law*, Intersentia, 2019.
- Marzocchi, O. and Mazzini, M., 'In-Depth Analysis for the Pegasus Committee: Pegasus and Surveillance Spyware', European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, May 2022.
- Moerel, L., and Prins, C., 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things', SSRN Scholarly Paper ID 2784123, 2016, available at https://papers.ssrn.com/abstract=2784123.
- Moscibroda, A., 'Law Enforcement Directive 2016/680: General principles and transposition', *Data Protection and the Law Enforcement Directive*, ERA Online Seminar, June 2020.
- Naudts, L., 'Criminal Profiling and Non-Discrimination: On Firm Grounds for the Digital Era?', *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructures*, Vedder, A. et al. (eds), 1st ed., KU Leuven Centre for IT & IP Law Series 7, Intersentia, Cambridge, Antwerp, Chicago, 2019, pp. 63–96.

- Naudts L., 'The Data Protection Impact Assessment for Law Enforcement Agencies', presented at the 12th International Conference on Communications, Bucharest, Romania, 15 June 2018.
- Oswald M., Grace, J., Urwin, S. and Barnes, G., 'Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality', *Information & Communications Technology Law,* Vol. 27, No. 2, 2018, pp. 223–50.
- Panteleeva, V., 'Transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 in Personal Data Protection Act in Republic Of Bulgaria', *Legal Science: Functions, Significance and Future in Legal Systems II*, The 7th International Scientific Conference of the Faculty of Law of the University of Latvia, 16–18 October 2019, Riga, Collection of Research Papers, pp. 210-217.
- Purtova, N., 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' *International Data Privacy Law*, Vol 8, No 52, 2018, pp. 52-68.
- Quezada Tavárez, K., 'Highlights of the Spanish Act on Data Protection in the Area of Police and Criminal Justice (Organic Law 7/2021)', CiTiP Blog,15 June 2021, available at https://www.law.kuleuven.be/citip/blog/highlights-of-the-spanish-act-on-data-protection-in-the-area-of-police-and-criminal-justice/.
- Quezada Tavárez, K., 'Impact of the Right of Access on the Balance between Security and Fundamental Right: Informational Power as a Tool to Watch the Watchers', *European Data Protection Law Review*, Vol. 7, No. 1, 2021, pp. 59–73.
- Quezada-Tavárez, K., Vogiatzoglou, P. and Royer, S., 'Legal Challenges in Bringing AI Evidence to the Criminal Courtroom', *New Journal of European Criminal Law*, Vol. 12, No. 4, 2021, pp. 531-551.
- Raab, C., 'Information privacy, impact assessment, and the place of ethics', *Computer Law & Security Review*, Vol. 37, 2020.
- Radtke, T., 'The Concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in Contrast to the GDPR', Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Vol. 11, No. 3, 2020, pp. 242-251.
- Renda, A., In-Depth Analysis requested by the JURI committee, 'Assessment of current initiatives of the European Commission on better regulation', Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 734.766, June 2022
- Rijpma, J. et al. (eds), *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, the XXIX FIDE Congress in The Hague 2020 Congress Publications, vol. 2, Eleven International Publishing, the Hague, 2020.
- Ripoll Servent, A., 'Protecting or Processing? Recasting EU Data Protection Norms' in Schünemann, W.J. and Baumann, M.O., (eds), *Privacy, Data Protection and Cybersecurity in Europe*, Springer 2017.
- Sajfert, J. and Quintel, T., 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', 1 December 2017, available at SSRN: https://ssrn.com/abstract=3285873.
- Sartor, G., In-Depth Analysis requested by the JURI committee, 'The way forward for better regulation in the EU – better focus, synergies, data and technology', Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 736.129, August 2022.

- Stephan S., 'Greenland, the Faroes and Åland in Nordic and European Co-operation – Two Approaches towards Accommodating Autonomies', *International Journal on Minority and Group Rights*, Vol. 24, No. 3, 2017.
- Trilateral Research, 'Human intervention and human oversight in the GDPR and AI Act', available at: https://trilateralresearch.com/research-highlights/human-intervetion-in-gdpr-and-ai
- Vogiatzoglou, P. and Fantin, S., 'National and Public Security within and beyond the Police Directive', *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructures*, Vedder, A. et al. (eds), 1st ed., KU Leuven Centre for IT & IP Law Series 7, Intersentia, Cambridge, Antwerp, Chicago, 2019, pp. 27–62.
- Vogiatzoglou, P., Quezada Tavárez, K., Fantin, S. and Dewitte, P., 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives', *Journal of Intellectual Property, Information Technology and E-Commerce Law,* Vol. 11, No 3, 2020, pp. 274–302.
- Vogiatzoglou, P., 'Article 2: Scope', *The Law Enforcement Directive: A Commentary*, Kosta, E. and Boehm, F. (eds), Oxford University Press 2022 (forthcoming – under review).
- Wandall, R., Ensuring the rights of EU citizens against politically motivated Red Notices', European Parliament Committee on Civil Liberties (LIBE), February 2022.
- Wenderhorst, C.and Duller, Y. 'Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces', PE 696.968, 2021.
- Winter, H.B. et al, *De verwerking van politiegegevens in vijf Europese landen*, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, November 2020.

EU and national institutions

- An Coimisinéir Cosanta Sonraí – Data Protection Commission (Irish supervisory authority), 'Law Enforcement Directive, Guidance on Competent Authorities and Scope', available at https://www.dataprotection.ie/en/organisations/resources-organisations/law-enforcement-directive.
- Article 29 Data Protection 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 or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015.
  Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017.
  Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', WP248, 2017.
  Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Greek supervisory authority), Γνωμοδότηση 1/2020 (Opinion 1/2020), Athens 24 January 2020.

- Commission Expert Group:

  Minutes of the first meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 23 September 2016
  Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 November 2016

Minutes of the fifth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 18 January 2017
Minutes of the seventh meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 March 2017
Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4 May 2017

- Commission nationale de l'informatique et des libertés (French supervisory authority):

  '"Law Enforcement Directive": What Are We Talking About?', 2 June 2021, available at: https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about.
  'Privacy Impact Assessment 1 (Methodology), 2 (Templates) and 3 (Knowledge bases)', July 2015, available at: https://www.cnil.fr/en/privacy-impact-assessment-pia.

- Commission nationale pour la protection des données (Luxembourgish supervisory authority), 'Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7168 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification de certaines lois, Délibération n° 1049/2017 du 28 décembre 2017.

- Council position and findings on the application of the 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, 13943/21, 18 November 2021.

- European Commission:

  Commission Staff Working Document Better Regulation Guidelines, SWD(2021) 305 final, 3 November 2021.
  Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, 25.7.2022, p. 16-18.

- European Data Protection Board:

  'Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive', 2 February 2021.
  'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures', 10 November 2020.
  Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, 14 December 2021.

  'Statement 02/2022 on personal data transfers to the Russian Federation', 12 July 2022.

- European Data Protection Supervisor:

  'Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters', COM(2005)475, 2006.
  'Opinion on the Data Protection Reform Package', 12 March 2012.
  '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', 28 October 2015.
  'Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation', 19 July 2019.

Opinion 8/2021 on the Recommendation for a Council decision authorising the opening of negotiations for a cooperation agreement between the EU and INTERPOL', 25 May 2021.
Preliminary remarks on modern spyware, 15 February 2022.
Press Statement 'Amended Europol Regulation weakens data protection supervision', EDPS/2022/16, 27 June 2022.

- EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021
- European Parliament, 'Recommendation of 5 July 2022 to the Council and the Commission on the negotiations for a cooperation agreement between the European Union and the International Criminal Police Organization (ICPO-INTERPOL)', 2022/2025(INI), 5 July 2022.
- European Union Agency for Fundamental Rights (FRA), *Handbook on European Data Protection Law*, 2018 edition, Publications Office of the European Union, Luxembourg, 2018, p. 291-324.
- European Union Agency for Network and Information Security (ENISA), 'Guidelines for SMEs on the Security of Personal Data Processing', 2016.
- EUROPOL, 'From Suspicion to Action - Converting Financial Intelligence into Greater Operational Impact', Publications Office of the European Union, Luxembourg, 2017.
- Information Commissioner's Office (ICO), 'Guide to Law Enforcement Processing', 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.
- The Romanian National Supervisory Authority for Personal Data Processing, 'Guidelines on the Application of Law No. 363/2018', https://www.dataprotection.ro/servlet/ViewDocument?id=2127.

ANNEX: LIST OF NATIONAL LAWS AS REVIEWED BY BIBLIOGRAPHIC SOURCES

Austria:

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG, 25 May 2018).

Belgium:

Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. 5 september 2018)
Wet van 5 augustus 1992 op het politieambt (Wet Politieambt) (B.S. 22 december 1992)

Cyprus:

Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα από Αρμόδιες Αρχές για τους Σκοπούς της Πρόληψης, Διερεύνησης, Ανίχνευσης η Δίωξης Ποινικών Αδικημάτων ή της Εκτέλεσης Ποινικών Κυρώσεων και για την Ελεύθερη Κυκλοφορία των Δεδομένων Αυτών Νόμος του 2019 (Cyprus Gazette 4694 p. 267, 27 March 2019)

Czech Republic:

Zákon ze dne 12. března 2019 o zpracování osobních údajů (Aktuální znění 24.04.2019)

Germany:

Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626)
Bundesgrenzschutzgesetz 1994

Greece:

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις (Εφημερίς της Κυβερνήσεως Α137 p. 03379; 29 August 2019).

Italy:

Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15 (Gazzetta Ufficiale della Repubblica Italiana 61, 14 March 2018)
Attuazione della direttiva UE 2016/680 del Parlamento Europeo e del Consiglio, del 27.4.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Gazzetta Ufficiale della Repubblica Italiana 119, 24 May 2018)

Ireland:

Data Protection Act 2018 (Act 7 of 2018) (Iris Oifigiúl 42 p. 00752, 24 May 2018)

Luxembourg:

Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale (Journal officiel du Grand-Duché de Luxembourg A 689 p. 1, 16 August 2018)

Netherlands:

Wet van 21 juli 2007 houdende regels inzake de verwerking van politiegegevens (Wet Politiegegevens, Stb. 2007, 549)
Raad van State Explanatory Memorandum on the Implementation of the LED, https://www.raadvanstate.nl/publish/pages/108235/w-16-17-0366.pdf
Wet van 7 september 2000 houdende Justitiële en Strafvorderlijke gegevens (Wet Justitiële Gegevens, Stb. 2004, 129)

Poland:

U S T AWA z dnia 14 grudnia 2018 r.o ochronie danych osobowych przetwarzanych w zwi±zku z zapobieganiem i zwalczaniem przestępczo

Portugal:

Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Diaro da Republica 151 p. 41, 8 August 2019)

Spain:

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (Boletín Oficial del Estado 126/2021-05-27, p. 64103)

This study analyses the main provisions of the Law Enforcement Directive as well as their implementation within national laws. In that context, the study identifies shortcomings and explores potential ways forward through a concrete set of recommendations.

This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Civil Liberties, Justice and Home Affairs.

PE 671.505
IP/C/LIBE/IC/2021-109

Print ISBN 978-92-846-9935-3 | doi:10.2861/272959 | QA-03-22-157-EN-C
PDF ISBN 978-92-846-9934-6 | doi:10.2861/691965 | QA-03-22-157-EN-N