The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680

Leiser, M.R.; Custers, B.H.M.

THE LAW ENFORCEMENT DIRECTIVE: CONCEPTUAL CHALLENGES OF EU DIRECTIVE 2016/680

Abstract

Passed in synchronicity with the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED – EU Directive 2016/680) has been heralded for its role in building "an area of freedom, security and justice with a high level of data protection, in accordance with the EU Charter of Fundamental Rights". Data processed for 'law enforcement purposes' by 'competent authorities' must comply with principles of necessity, proportionality & legality, while ensuring appropriate safeguards in place for data subjects. Despite an increase in scope, applicability, and rights and freedoms of individuals, there is ambiguity as to how the LED should work in practice. This is due to several conceptual issues that the LED raises.

This paper discusses three of these issues. The first concerns the role of consent in the LED. Although the LED uses consent as a central concept, this is fundamentally at odds with the processing of personal data in a law enforcement context. The second issue is that the LED requires competent authorities to categorize data relating to witnesses, suspects, and victims. This is problematic, because a participant's role in a criminal event is both fluid and dynamic and the roles of data subjects typically change over time or sometimes even overlap. The third issue is that the LED requires competent authorities to document whether data collected is a 'fact' or an 'opinion'. The problem here is that 'factual' accounts of witnesses and others are always inherently subjective. The LED´s requirement on competent authorities to categorize facts from opinions and for controllers to make a clear distinction between offenders, suspects, witnesses, and victims puts recognized data protection principles of lawfulness, fairness, transparency in the crosshairs. Together, these three issues create a consent and categorization quagmire.

It is concluded that, while in some respects the LED brings data controller obligations for law enforcement authorities into the 21st Century, the LED contains conceptual issues and, in comparison to the GDPR, contains limited transparency requirements, lower thresholds for consent, and, in some areas, lower standards for protecting data subject rights. When the goal is to offer better protection for data subjects, a focus on transparency and clear data processing limitations for data controllers may be more suitable than the suggestive concepts of consent and control that are hardly enforceable for data subjects.

Introduction[1]

Recent developments in EU data protection law have dominated headlines and regulatory discourse about how to implement and comply with the General Data Protection Regulation[2] (hereafter, GDPR).[3] With comparatively little fanfare, the parallel, *lex specialis,*[4]

[1] Authors' bio to be reentered here. Part of this paper is based on research performed in the EU project xxxxxx, on the xxx, grant number xxx

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

[3] P de Hert and J Sajfert, 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data' in C Brière and A Weyembergh (eds), The needed balances in EU Criminal Law: past present and future

[4] Note that, depending on the perspective, the LED can be considered as a regime parallel to the GDPR or as a lex specialis applicable to law enforcement.

Directive (EU) 2016/680 on protecting personal data processed for the purposes of law enforcement[5] entered into force at the same time, with the stated aim of ensuring EU Member States "protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".[6] The EU Parliament exercised its legislative powers[7] to enact Directive 2016/680 on processing personal data for police and judicial matters (hereafter, LED), and for international transfers, repealed the 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.[8] With advances in technology and processing capabilities[9] at the heart of its justification, the EU Parliament set about implementing a comprehensive approach to data protection regulation across almost all sectors of the EU community.[10] Political consensus was found through trilogue negotiations, with the EU Parliament emphasizing a 'package' approach to ensure that the GDPR and the LED were dealt with in parallel.[11]

The LED covers activities by "competent authorities" for the "prevention, investigation and prosecution of criminal offences".[12] The scope of the LED has been extended to cover prevention of threats to *public*, but not *national* security, while providing new rights for data subjects[13] as well as new obligations[14] for "competent authorities" processing data for "law enforcement purposes", i.e., 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".[15]

Despite an increase in scope, applicability, and rights and freedoms of individuals, there is ambiguity as to how the LED should work in practice. Unlike the GDPR (an EU Regulation is directly applicable to all EU residents in all EU Member States), the LED is an EU Directive, requiring transposition into national law of all EU Member States. The cut-off date for implementation was in May 2018, but many EU Member States had issues meeting that deadline.[16] The implementation into national legislation and the execution by competent authorities raises several issues. This is due to both conceptual and practical issues that the LED raises, which are discussed in this paper.

From a conceptual perspective, three issues are discussed. The first issue concerns the role of consent in the LED. Although the LED uses consent as a central concept, this is fundamentally at odds with the processing of personal data in a law enforcement context. The

---

[5] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89.
[6] Article 1(2)(a) LED
[7] Article 16(2) of the Treaty on the Functioning of the European Union (TFEU)
[8] Recitals 4, 7, LED.
[9] Recital 3, LED.
[10] Recital 14, LED. See also Custers B.H.M. & Vergouw S.J. (2015), Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies, *Computer law & security report* (31): 518-526; Custers B.H.M. (2012), Technology in Policing: Experiences, Obstacles and Police Needs, *Computer law & security report* (1): 62-68.
[11] For a very good overview of the Law Enforcement Directive, see Sajfert, Juraj and Quintel, Teresa, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3285873
[12] Article 1, LED.
[13] These include Right of access by the data subject (Article 14), Right to rectification or erasure of personal data (Article 16), Right to receive information by the data subject (Article 13).
[14] These include obligations to log (Article 25), Data protection by design and default (Article 20), appoint a data protection officer (Article 32)
[15] Ibid.
[16] Some Member States, like Germany, Denmark, Ireland and Austria adopted national legislation implementing the directive before this deadline. Other Member States, like the Netherlands, Belgium, Finland and Sweden did not meet the deadline, but have implemented the directive end 2018 or early 2019. Some other Member States, like Spain, France, Latvia, Portugal and Slovenia have not yet implemented the directive. For a complete overview, see http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30309.

second issue is that the LED requires competent authorities to categorize data relating to witnesses, suspects, and victims. This is problematic, because a participant's role in a criminal event is both fluid and dynamic and the roles of data subjects typically change over time or sometimes even overlap. The third issue is that the LED requires competent authorities to document whether data collected is a 'fact' or an 'opinion'. The problem here is that 'factual' accounts of witnesses and others are always inherently subjective. The LED´s requirement on competent authorities to categorize facts from opinions and for controllers to make a clear distinction between offenders, suspects, witnesses, and victims puts recognized data protection principles of lawfulness, fairness, transparency in the crosshairs.

From a practical perspective, the national implementation in EU member states raises issues. This is illustrated by examining the UK and Dutch approaches to the concept of consent, a fundamental and controversial aspect of data protection law. First, the fallout is examined from the planned rollout of 'cyber kiosks' by Scotland's centralized law enforcement agency, Police Scotland, whose own data protection impact assessment (DPIA) revealed the organization may not have processed personal data for law enforcement purposes lawfully, fairly, and transparently. The DPIA revealed Police Scotland was not transparent about processing personal data after obtaining consent from data subjects and the entire legal basis for processing personal data for law enforcement purposes may not have been fit for purpose. Second, the Dutch perspective is examined, in which the Police Data Act did not require major changes, but nevertheless lacks proper practical implementation and enforcement.

This paper is structured as follows. Section 2 provides some background information on the LED, including a brief overview of the LED's scope, applicability, data subject rights, and data controller obligations. Section 3 examines three conceptual issues, i.e., consent and control, data subject categorization, and facts versus opinions. Section 4 provides conclusions.

2. Background of the LED

The LED aims to set more specific rules for the processing in personal data in law enforcement. This domain is explicitly excluded from the scope of the GDPR (see article 2.1.d of the GDPR). Although information rights exist in law enforcement, as will discussed below, the balance between the needs of law enforcement organizations and the protection of data subjects is slightly different in law enforcement than regulated by the GDPR. The LED tries to provide this more contextualized balance.[17] At the same time, on a more general level, the LED constitutes a further harmonization of law enforcement across EU member states, facilitating the cooperation within the EU in the area of law enforcement. As such, the LED is not only about ensuring the same level of protection for natural persons, but also about the free movement of data.[18] In this section we discuss the history of the LED (subsection 2.1), its material scope and terminology (section 2.2), and principles for data processing (subsection 2.3). This section can only provide a brief overview, for more detailed accounts, we refer to existing literature.[19]

2.1 History

The history of LED runs mostly parallel with that of the GDPR. The GDPR mainly builds on and extends the EU Data Protection Directive (DPD) from 1995.[20] This Directive, in

[17] Nadia Purtova (2017), 'Between GDPR and the Police Directive: Navigating through the maze of information sharing in Public-Private Partnership' available at SSRN: https://ssrn.com/abstract=2930078.
[18] See Recital 15 of the LED.
[19] Juraj Sajfert and Teresa Quintel, Data Protection Directive (EU) 2016/680 For Police And Criminal Justice Authorities, Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873, Accessed 31 March 2019; Paul De Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive, A first analysis", in: *New Journal of European Criminal Law*, Vol.7, Issue 1, 2016, p. 17. Paul De Hert and Vagelis Papakonstantinou 'Data protection policies in EU Justice and Home Affairs. A multi-layered and yet unexplored territory for legal research', in: Ariadna Ripoll Servent & Florian Trauner (eds), Routledge Handbook of Justice and Home Affairs Research, Routledge, London, 2018, 169-179.
[20] For further reading, see Bygrave, L.A. (2002) Data Protection Law; approaching its rationale, logic and limits, Information Law; *Kuner, C. (2012). The European Commission's proposed data protection regulation: A*

turn, was mostly based on the provisions in Convention 108 of the Council of Europe (also referred to as the Treaty of Strasbourg) from 1981.[21] The Council of Europe published a recommendation that supplements Convention 108 for the use of personal data by the police in 1987.[22] This recommendation specified who is permitted access to police data, under what conditions police data can be transferred to authorities in third countries, how data subjects can exercise their data protection rights and how independent supervision is organized. Those recommendations, however, were not legally binding and many member states have not fully implemented them.

Since the processing of criminal law data is beyond the scope of Directive 95/46/EC, there was historically little harmonization within the EU.[23] After the September 11th terrorist attacks in the United States, the European Parliament repeatedly requested a legal instrument under the third pillar of the European Union, on Police and Judicial Cooperation in Criminal Matters.[24] However, little progress was made.[25] Only in 2008 did the EU publish Framework Decision 2008/977/JHA on the protection of personal data processing in the framework of police and judicial cooperation in criminal matters.[26] This Framework Decision was also based on Convention 108 and the Data Protection Directive principles. National security was beyond the scope of the Framework Decision. The aim of the Framework Decision is, on the one hand, the protection of personal data that are processed for the prevention, investigation, detection and prosecution of crimes and the execution of criminal penalties and, on the other hand, the facilitation and simplification of police and judicial cooperation between member states.

In this context, a series of other legal instruments aim to advance the cooperation and sharing of information between member states, such as the Prüm Treaty[27] (for exchanging DNA data, fingerprints and traffic data), the Schengen Information System[28] (SIS, for international criminal investigation information), the Visa Information System[29] (VIS), for visa data, including biometrical data), and the Customs Information System (CIS)[30]. Also the institutional regulations for Europol, Eurosur and Eurojust contain provisions for the exchange of criminal law information.

In 2012 the European Commission presented the first draft for a Directive that is much broader than the Framework Decision, that would harmonize the processing of personal data in criminal law matters.[31] After that, a debate started between the European Parliament, the Commission and the Council, which took four years. In 2016, the legislative proposal was adopted, after amendments, in its current version as EU Directive 2016/680. In this Directive the deadline for implementation in national legislation is two years, with a final deadline in

---

copernican revolution in European data protection law. Bloomberg BNA Privacy and Security Law Report (2012) February, 6(2012), 1-15.; Hornung G. (2012) A General Data Protection Regulation for Europe? Light and Shade in the Commission"s Draft of 25 January 2012, 9 *SCRIPTed* 64-81. Series 10, Den Haag: Kluwer Law International.

[21] Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108, 28.01.1981.

[22] Council of Europe (1987) Police Data Recommendation Rec(87)15, 17.9.1987.

[23] Pajunoja, L.J. (2017) The Data Protection Directive on Police Matters 2016/680 protects privacy - The evolution of EU´s data protection law and its compatibility with the right to privacy, Master Thesis, Helsinki: University of Helsinki.

[24] Pajunoja, L.J. (2017) The Data Protection Directive on Police Matters 2016/680 protects privacy - The evolution of EU´s data protection law and its compatibility with the right to privacy, Master Thesis, Helsinki: University of Helsinki.

[25] Gonzales Fuster, G. (2014) The Emergence of Personal Data Protection as a Fundamental Right of the EU. Heidelberg: Springer, p. 220.

[26] Europese Raad (2008) Framework Decision 2008/977/JHA, 27.11.2008

[27] EU Council Decision 2008/615/JHA; Prüm Decision, 23.6.2008.

[28] EU Council Decision 2007/533/JHA, SIS-II, 12.6.2007.

[29] EU Regulation 767/2008, VIS Regulation, 9.7.2008.

[30] EU Council Decision 2009/917/JHA.

[31] COM(2012) 10 Final, 2012/0010, Brussels 25.1.2012, Proposal or 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. Available at http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52012PC0010&from=en Accessed 19 Jan 2019.

May 2018. Directive 2016/680 (the LED) repeals the current Framework Decision 2008/977/JHA as of that date.

The aim of the LED is two-fold: it ensures the protection of personal data processed for the prevention, investigation, detection and prosecution of crimes and the execution of criminal penalties. It also facilitates and simplifies police and judicial cooperation between member states and, more in general, effectively addressing crime.[32] This two-pronged approach is similar to that of the GDPR and to the Framework Decision.

The most important differences between, on the one hand, the general legal instruments for the protection of personal data (Convention 108, the Data Protection Directive and the GDPR) and, on the other hand sector-specific legal instruments for the protection of criminal law data (Recommendation 87/15, Framework Decision 2008/977/JHA and Directive 2016/680) are: first, the scope and targeted audiences are different; and second, specific data subject rights are more restricted in criminal law matters and, third, the criminal law provisions offer a bit more detail for data processing, such as specific obligations for categorising data (Art. 6 and 7 of the LED Directive, see sections 3.2 and 3.3) and specific exceptions for courts (Art. 32 and 45 of the LED Directive).

2.2 Material scope and terminology

The scope and the objectives of the LED are presented in its first chapter,[33] together with a set of definitions explaining the terminology used. The LED's foundations recognize the protection of personal data is a fundamental right and freedom of natural persons and it lays the basis for ensuring the protection of the transfer of data among member states.

The LED focuses on data processing by 'competent authorities', as defined in Article 3(7). **Competent authorities** include:

> (a) 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, and;
>
> (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Perhaps the most obvious competent authorities are police forces and public prosecution services, but there may be a variety of competent authorities in national criminal law of EU member states. For instance, in the domain of execution of criminal penalties, competent authorities may include the 'regular' prison system, juvenile correction centers, forensic psychiatric centers, probation authorities, etc.[34]

The scope of the LED is limited to the processing of personal data by the competent authorities for the **specific purposes** of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[35] This includes the safeguarding against and the prevention of threats to public security.[36] As such, it should be noted that not all personal data processed by law enforcement agencies and the judiciary is within the scope of the LED. For instance, when law enforcement agencies or the judiciary are processing personnel data regarding their staff, for paying wages or assessing employee performance, the GDPR applies rather than the LED. The GDPR is also applicable for personal data processing regarding borders, migration and asylum.

[32] See also Recital 15 of the LED.
[33] Articles 1-3 of the LED.
[34] See also Recital 11 and 22 of the LED.
[35] Articles 1 and 2 of the LED.
[36] See also Recital 11 of the LED.

Both data used on crimes that have already taken place (for instance, data regarding crime reconstructions and evidence for in courts) and data used on crimes that still might take place (for instance, crime prediction models that police agencies use to prevent crime)[37] fall within the scope of the LED. Data is not limited to criminal events, but also to suspects, criminals, victims, witnesses, testifying law enforcement officers, and police informants. In case of crime prevention, there may be suspects involved (i.e., those preparing a crime), without a completed criminal act (as it was still in preparation).[38]

Article 4 LED provides a list of definitions. The definition of personal data is the most important.[39] Similar to the GDPR text, personal data is defined as any information relating to an identified or identifiable[40] natural person (the data subject). This means that data relating to legal persons (even when they are involved in criminal matters) are not within the scope of the LED. The processing of personal data includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. It should be noted that some types of data processing, such as anonymization,[41] may transform personal data into anonymous (i.e., non-personal) data, putting it beyond the scope of the LED.

2.3 Principles for data processing

The main substance of the LED, like the GDPR, consists of the 'fair principles' for the processing of personal data. These provide procedural rules and guidance for the processing of personal data, in order to ensure fairness. The principles for the processing of personal data include fair and lawful processing, purpose limitation, accuracy of the data, adequate security safeguards and responsibility of data controllers. The principle of transparency is observed as much as possible, but there are differences in the phrasing of the GDPR and the LED, because full transparency may not always be realistic in criminal law, as it may interfere with or frustrate ongoing criminal investigations. Hence, the basic idea of informational self-determination and data subjects' control over their own data in the GDPR also underpins the LED.[42]

The main principles for data processing reflect those in Convention 108 and the Data Protection Directive (see previous subsection) and include:[43]

- Lawfulness and fairness[44]
- Purpose specification and limitation[45]
- Data minimization[46]
- Accuracy[47]
- Storage limitation[48]

[37] See also Recital 26.
[38] Note that preparing serious crimes is a punishable offence (and hence a crime in itself) in most jurisdictions.
[39] See also WP29 (2018) Guidelines on Personal data breach notification under Regulation 2016/679. Article 29 Working Party, 6 February 2018; WP29 (2018) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Article 29 Working Party, 6 February 2018;
[40] Identifiability may depend on the amount of time, effort and costs involved. For more on absolute or relative identifiability of a person, see also ECJ, Case C-582/14 (Breyer/Germany).
[41] See also Article 3.5 of the LED.
[42] As elaborated further in Subsection 3.1, this is problematic.
[43] For further reading, see R. Gellman (2012) Fair Information Practices: A Basic History, available at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.
[44] Article 4.1.a
[45] Article 4.1.b
[46] Article 4.1.c
[47] Article 4.1.d
[48] Article 4.1.e

- Appropriate security[49]
- Accountability[50]

Personal data should be collected for specified, explicit and legitimate purposes within the LED's scope and should not be processed for purposes incompatible with 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.[51] Some of these principles are problematic, particularly when data are transferred from a GDPR regime into the context of law enforcement.[52] For instance, due to the different purposes and the recontextualization create ambiguity from a legal perspective. Also, the protection provided under the GDPR may decrease, from a data subject's perspective, when law enforcement agencies get access to data collected by private parties.[53]

Whereas the GDPR is not very specific about time limits for data storage and review[54], the LED requires clear establishment of time limits for storage and review.[55] The LED states that member states should provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Article 5(1)(e) GDPR states that personal data should be kept no longer than necessary, but does not mention a number of days, months or years. The Article 29 Working Party issued an opinion that argues that time limits should be differentiated.[56] Storage time limits vary across Member States and for different situations, including different types of data subjects and different crimep. For instance, in Germany, data storage duration is limited depending on the types of persons: ten years for adults, five years for adolescents and two years for children.[57] Data on whistle-blowers and informants can only be stored for one year, but can be extended to three years. For instance, in the Netherlands the storage of personal data by the police is limited to one year, which can be extended to five years if the data are necessary for the police tasks.[58] In the United Kingdom, Section 39(2) of the Data Protection Act 2018 requires that appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

Unlike the GDPR, the LED explicitly distinguishes different categories of data subjects. Article 6 requires competent authorities to distinguish between suspects, persons convicted of a crime, victims and other parties to a criminal offence (including witnesses). Data controllers, therefore, should make clear distinctions between the personal data of different categories of data subjects.

A third difference between the GDPR and the LED is that the latter requires competent authorities to register facts and opinions separately. Article 7 LED states personal data based

---

[49] Article 4.1.f
[50] Article 4.4
[51] If personal data are processed by the same or another controller for a purpose within the scope of the Directive other than that for which it has been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose; See Recital 29.
[52] Jasserand, C. (2018). Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation? . *European Data Protection Law Review* , 4(2), 152-167. https://doi.org/10.21552/edpl/2018/2/6.
[53] Jasserand, C. (2018). Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in Directive 2016/680? *Computer Law & Security Review*, 34(1), 154-165. https://doi.org/(...)6/j.clsr.2017.08.002.

[54] Article 5.1.e of the GDPR states that personal data should be kept no longer than necessary, but does not mention a number of days, months or years. Note that Articles 13 and 14 of the GDPR requires data controllers to inform data subject on storage times if they inquire about this.
[55] Article 5 of the LED. See also Quintel, T.A. (2018) European Union – Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive. *European Data Protection Law Review*, 4(1), p. 104-109.
[56] WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.
[57] Art. 35 Bundesgrenzschutzgesetz 1994
[58] Art. 8 Wet Politiegegevens

on facts to be distinguished as far as possible from personal data based on personal assessments.

Data subject right	Directive 2016/680	GDPR
Right to information	Art. 12-14	Art. 12-14
Right to access	Art. 14-15	Art. 15
Right to rectification	Art. 16	Art. 16
Right to erasure (right to be forgotten)	Art. 16	Art. 17
Right to restriction of processing	Art. 16	Art. 18
Right to data portability	N/A	Art. 20
Right to object to automated individual decision-making	N/A	Art. 21-22

Based on the concept of informational self-determination and data subject control over personal data, the LED contains a list of data subject rights and data controller obligations. These rights and obligations aim to provide further protection and control for data subjects, via, inter alia, transparency and consent. A list of data subject rights and data controller obligations is provided in Table 1 and Table 2 respectively.

Table 1 *Overview of data subject rights in Directive 2016/680 vs the GDPR*

Table 2: *Overview of data controller obligations in Directive 2016/680 vs the GDPR*

Data controller obligation	Directive 2016/680	GDPR
Data protection by design	Art. 20	Art. 25
Data protection by default	Art. 20	Art. 25
Maintain records	Art. 24	Art. 30
Logging	Art. 25	N/A
Cooperation with the DPA	Art. 26	Art. 31
Data protection impact assessment	Art. 27	Art. 35
Security of processing	Art. 29	Art. 32
Data breach notification	Art. 30-31	Art. 33-34
Prior consultation with the DPA	Art. 28	Art. 36

Data protection officers	Art. 32-34	Art. 37-39

3. Conceptual issues

The structure, terminology, and concepts in the LED run in parallel with those of the GDPR. The GDPR is based a conceptualisation of informational privacy that focuses on 'informational self-determination'[59] or 'privacy as control'.[60] In essence, this means that individuals should be in control over who collects and processes their personal data and for which purposes. For the GDPR this makes sense, as it empowers citizens in the data economy.[61] The empowerment of citizens is shaped via provisions for transparency, consent and data subject rights. From the viewpoint that suspects and other actors in criminal law should have rights and protection against competent authorities like law enforcement agencies, it makes sense to also ensure transparency and data subject rights in a criminal law context. However, as will be discussed below, concepts like consent and (full) transparency may not always be realistic in criminal law, as it may interfere with or frustrate ongoing criminal investigations. In this section, we discuss the conceptual issues of the LED related to this. First, the issue of consent and control is discussed (Subsection 3.1), next the categorisation of data subjects is examined (Subsection 3.2), and finally the distinction between facts and opinions is discussed (Subsection 3.3).

3.1 Consent and control

Article 6 of the GDPR contains six different legal bases for the lawful processing of personal data. The first one is (informed) consent, the other five involve situations in which data processing is necessary, for instance, necessity to perform a contract, to comply with a legal obligation, or to protect vital interests of data subjects. The LED only contains one legal basis for the processing of personal data, which is the necessity for the performance of the tasks of competent authorities in a criminal law context.[62] In other words, consent is not required and not even a potential legal basis for processing personal data under the LED. This makes sense particularly for suspects of a crime, who may not be willing to consent to the processing of their data, although such data processing is necessary for law enforcement agencies do their job. However, it may be less obvious for other data subjects in criminal law, such as witnesses or victims, who may expect that they have the opportunity to provide or withhold consent, particularly when they voluntarily contacted the police.

The LED embraces concepts of consent and control (and related concepts like transparency). The most relevant are the data subject rights (see Table 1) that the LED offers. Contrary to the data controller obligations in Table 2, which provide data subjects with a more protective and perhaps even paternalistic regime, the LED's data subject rights focus on empowerment and control that data subjects have. In particular, the right to have data deleted and the right to restrict processing of the data provide data subjects with more control. Furthermore, the right to information and the right to access aim to ensure that any consent

[59] See the ruling of the German Constitutional Court of 1983, BVerfGE 65, 1 at http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintText&Name=bv065001, which first established this concept in the EU. For an earlier account, from the United States, see Westin, A. (1967) *Privacy and Freedom*, London: Bodley Head.

[60] Lawrence Lessig, "Code And Other Laws Of Cyberspace 143 (1999): "Privacy, as Ethan Katsh defines it, is the power to control what others can come to know about you."; See also Paul M. Schwartz, Internet Privacy and the State, 32 CONN. L. REv. 815 (2000) and Solove, D. (2004) *The Digital Person; Technology and Privacy in the Information Age*, New York: University Press at Page 240 citing Randall P. Bezanson, "The Right to Privacy Revisited: Privacy, News, and Social Change, 80 Calif. L. Rev. 1133, 1135 (1992): "I will advance a concept of privacy based on the individual's control of information . . ."

[61] Custers B.H.M. & Bachlechner D. (2017), Advancing the EU Data Economy: Conditions for Realizing the Full Potential of Data Reuse, *Information Polity* 22(4): 291-309.

[62] Article 8 LED.

is also informed consent, as they allow data subjects to learn more about how the data collecting and processing takes place.

Obviously, data subject rights under the LED are more limited than under the GDPR. This may be a satisfactory state for data processing by law enforcement authorities, but the regime has friction between data subject control and empowerment and the limits to that control and empowerment inherent in the LED. There is nothing wrong with protecting fundamental rights of people who are subjected to or involved in a criminal investigation, but the suggestion (via the introduction of data subject rights) that they are in control and can consent or object to the processing of their data is misleading.

Looking at the LED, suspects of a crime have limited means of exercising their data subject rights, as this would interfere with criminal investigations. For those convicted, this is not very different, as it would interfere with the execution of criminal penalties. It may be argued that victims and witnesses have a choice to contact law enforcement agencies, but after they have done so, their means of influencing the data processing are limited.

The data subject rights in the GDPR suffer from practical problems, such as (1) limited awareness among data subjects on who is processing their personal data, which data, and for which purposes, (2) limited awareness on data subject rights they have, and (3) limited awareness on how to exercise these data subject rights.[63] The practical issues are even more prominent in a law enforcement context, in which people may sometimes not know that they are subject of a criminal investigation or, if they know, may not be able to invoke these data subject rights. As a result, it may be argued that data subject rights and the concepts of consent and control are a bit misleading. When the protection of data subjects in a democratic society is the goal, transparency and clear restrictions for data controllers seem to be more suitable for the law enforcement context than a focus on data subject rights that may be hard to invoke and effectuate by data subjects.

3.2 Categorisation of data subjects

The LED requires competent authorities to categorize personal data of data subjects, where applicable and as far as possible, as either a suspect, a person convicted of a criminal offence, a victim, a witness, an expert, and/or a person of interest or holding relevant information.[64] The Directive's approach to categorization is surprisingly unjustified in the Recitals, with the only caveat to the requirement that categorization should "not prevent the application of the right of presumption of innocence as guaranteed by the Charter and by the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively."[65]

Categorizing data this way is intrinsically linked to requirements on Member States to legislate time limits for the maximum storage period for certain categories of data and timeframes for periodic review thereof.[66] Using principles of necessity and proportionality as justification, the LED requires each Member State to ensure existing and future databases automatically delete or anonymise "as soon as the deadline for data storage has been reached".[67] The Article 29 WP Guidance goes even further in its recommendations, stating that

[63] Eurobarometer Survey 431 (2015). *Attitudes on Data Protection and Electronic Identity in the European Union*. Brussels, June; Solove, D.J. (2013) "Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126: 1880–903; Adjerid, I., A. Acquisti, L. Brandimarte and G. Loewenstein (2013) "Sleights of Privacy: Framing, Disclo- sures, and the Limits of Transparency," *Proceedings of the Ninth Symposium on Usable Privacy and Security*. Newcastle, 24–6 July. New York: ACM; Acquisti, A. (2009) "Nudging Privacy: The Behavioral Economics of Personal Information," *Security & Privacy Economics* 7(6): 72–5; Custers, B. (2016) "Click Here to Consent Forever: Expiry Dates for Informed Consent," *Big Data and Society*, January–June 2016: 1–6. doi: 10.1177/2053951715624935.

[64] Article 6 LED.

[65] Recital 31.

[66] Article 5 LED.

[67] European Data Protection Supervisor, "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit", 11 April 2017, Available at https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en, Accessed 31 March 2019.

in the event of failure by the controller to conduct a periodic review of whether further processing is necessary, then data should be automatically deleted or pseudonymised.[68] Competent authorities must, therefore, periodically review data held. This review should objectively analyse whether continuing to hold data makes an effective contribution for the purposes pursued and must objectively determine the length of the maximum storage period or periodic review to achieving that purpose.

The categorization requirement may be *conceptually* in-line with the jurisprudence of the ECtHR[69], and the practice of attaching different codes to categories of data has been already developed and in use;[70] however, there are some fundamental issues and concerns about the concept. First, this categorization requires making complicated decisions on how to typify actors in a crime. Criminal events are rarely witnessed by law enforcement first-hand and sometimes initial observations are misguided, confusing, and/or wrong. Nevertheless, a decision has to be made when registering the personal data. Second, the categorization is static, while process of criminal investigation is both fluid and dynamic. For instance, a victim may turn out to be the perpetrator[71,72] Third, some roles may overlap: a stabbing victim may also be a witness to an event;[73] A victim may also be a perpetrator. This is not just pedantry. Mendelsohn's influential typology of criminal victims categorizes six types of victims ranging from completely innocent victims at one end of the spectrum to guilty and imaginary victims at the other.[74]

The practice can be traced back to the creation of Europol, an organization created with the major objective of improving the sharing of intelligence about transnational crime that between Member States.[75] It does not engage in law enforcement directly, but facilitates sharing of information, notifying Member States when intelligence analysis reveals "information concerning them and of any connections identified between criminal offences", provide "strategic intelligence" and "general situation reports", and collect shared intelligence on terrorism.[76] Article 6 of the Convention provides the legal basis for the creation of a "computerized system of collected information" with strict rules over access to and limits on the types of information that can be entered into the database.[77] The Convention also requires Europol to code the information entered as either coming from a third party or as "the result of its own analyses".[78]

Although the Law Enforcement Directive mandates categorization in itself, the concept of categorization found in Article 29 of the Europol Regulation[79] requires coding relative to an assessment of the *quality* of a source and the *accuracy* of their information. The mechanism is used to inform one Member State receiving intelligence from another with a qualitative assessment; thus, adding a classification code does nothing more than enable a competent authority to gauge what value it should attach to the information transferred. Europol uses a mechanism called an Analysis Work File (AWF) for operational collaboration among law enforcement agencies across the EU. Data relating to specific criminal phenomena like human

[68] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", 29 November 2017, Available at https://iapp.org/media/pdf/resource_center/wp258_police_directive-11-2017.pdf, Accessed 31 March 2019.
[69] See ECtHR App nos 30562/04 and 30566/04 *S and Marper* v United Kingdom (4 December 2008) .
[70] Article 29 of the Europol Regulation (EU) 2016/794.
[71] For an example, see https://www.bbc.com/news/world-europe-47879648.
[72] Turvey, B. E. (2013). Forensic fraud: Evaluating law enforcement and forensic science cultures in the context of examiner misconduct. Academic Press.
[73] For an example, see https://metro.co.uk/2019/04/10/witness-stabbed-back-filming-knife-attack-dad-son-9142161/.
[74] Sengstock, M. C. (1976). The Culpable Victim in Mendelsohn's Typology.
[75] For a list of activities in which Europol see page 192 of Occhipinti, J. (2003) The Politics of EU Police Co-operation: Towards a European FBI? (Boulder, CO: Lynne Rienner).
[76] Article 3(2) and Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention).
[77] Article 7 and Article 9 of the Europol Convention.
[78] Article 8(3).
[79] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11th May 2016.

trafficking and money laundering is analyzed in one comprehensive environment; thus, data relating to criminals, associates, witnesses, victims, and informants can be viewed in a dedicated environment.[80] Unsurprisingly, there are extremely tight controls in place for accessing information.[81] In order to ensure the authenticity of the information shared across law enforcement authorities, the data is routinely checked for its validity and accuracy and tagged with a marker for different purposes; for example, excluding access.[82] Data within AWF is analyzed, graded, and assessed for quality by experts so that other law enforcement agencies can make informed decisions about how much weight to give to it. In this case, categorization facilitates how much trust to place in shared intelligence.

Unlike the Europol framework, Article 6 LED has the effect of attaching categories to data and then linking those categories to *specific* time limits for deletion is problematic. Victims of crime can quickly become suspects. Suspects can become victims. Accused can quickly become either convicted or exonerated. Some accusations are not seen as prosecutable until corroborative evidence is provided from other victims. Terminology is important in criminal law; and victims are no longer seen and treated as passive actors in the criminal justice system. The English case of *R v Ahluwalia*[83] is a prime example of how dynamic and fluid actors can be. Ahluwalia was the victim of domestic abuse over a period of ten years, was suspected of killing her husband, and was convicted of murder. On appeal three years later, her conviction was overturned after she was found not guilty by diminished responsibility in her retrial. Unlike the Europol approach, which focuses on sharing the value in the integrity of the data, categorization under the LED must not only be dynamic, but updating as new facts emerge during an investigation. This requirement could disproportionately affect certain categories of crime such as historical sex abuses and cold cases, wherein it is not possible to immediately compile enough evidence to corroborate the allegations made by a complainer until new, additional data satisfies the sufficiency of evidence tests.

3.3 Facts vs opinions

Article 7 requires Member States provide for personal data based on *facts* to be distinguished from personal data based on *opinions*. Article 7(2) requires "all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available". This ensures competent authorities must put in practices that ensure the "quality, accuracy, completeness and reliability of personal data have to be verified and properly indicated before data exchanges with other authorities may take place".[84] Data subjects have the right of rectification of inaccurate personal data relating to them,[85] in particular, when it relates to facts.[86] Taking into account the purposes of the processing, data subjects also have the right to have incomplete data completed, including by means of providing a supplementary statement.

While recognising that the processing of inaccurate data by competent authorities within the scope of the Directive might have adverse effects on data subjects, the requirement to rectify any inaccuracies with the necessary urgency could also adversely affects certain classes of data subjects. As data subjects become more aware of their rights, and with the particular sensitivities around criminal investigations and proceedings, vigilance will be needed at achieving the balance between competing data subject rights and other participants in a criminal event. A police office will rarely witness an incident first-hand. Upon investigation of a criminal complaint, statements may be taken and observations made; however, this does not mean they are truthful statements or that complaints are documented

[80] Art. 6 AWF Rules.
[81] Art. 5 AWF Rules.
[82] Art. 14 (6) of The Europol Council Decision (ECD).
[83] [1992] 4 All ER 889.
[84]Juraj Sajfert and Teresa Quintel, Data Protection Directive (EU) 2016/680 For Police And Criminal Justice Authorities, Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873, Accessed 31 March 2019.
[85] Article 16(1).
[86] Recital 47.

accurately. Observations might lead to conclusions or even inferences, but it does not mean they are correct.

Courts treat facts and opinions differently because they do different things to their audiences – facts educate, while opinions influence. In light of this, the rationale for distinguishing between facts and opinions suggests there is some intrinsic method for doing so: assessment of either's effect on its audience. On the contrary, a defamatory statement – which might be either a fact or opinion – is determined by an objective, common sense perspective by an average member of the public.[87]

The distinction between facts and opinions in the Directive suggests that there is a clear rationale for labelling data in both categories. Facts are anything directly observed or checked for accuracy. However, a clear problem is constituted by inferred data,[88] such as risk profiles, likely offenders, or recidivism risks, for which there is no categorization. These are not opinions, but characteristics derived from data analytics and ascribed to individuals. Neither are inferred data facts, in the sense of directly observable characteristics or characteristics that can (easily) be checked for accuracy. Inferred data are often probabilities or estimates, which have different levels of reliability than facts.[89]

Currently the Directive states that all personal data recorded that is not a fact (included inferences) must be logged as merely an opinion. An inference, far less reliable than a fact, is a derived logical conclusion from something directly observed; however, an opinion may not naturally follow on from the facts. For example, a traffic officer's claim that a driver was speeding is only an opinion. Noting that a radar gun displayed a readout that indicated the driver was travelling over 70 miles an hour is a fact. Claims that the driver was speeding based on a factual reading of the radar gun display is an inference. However, the person making the inference may not have all the evidence to make a proper inference; for example, it may be permitted for the driver to travel at that speed. Thus, factual claims that a data subject was speeding would be subject to rectification under Article 16(2). Accordingly, controllers must determine what personal data must be maintained for the purpose of evidence. Where the accuracy of personal data is contested by a data subject and the accuracy of that data cannot be determined, Recital 47 foresees the right to obtain a restriction of processing via technical means instead of erasure by the controller:

> "Methods to restrict the processing of personal data could include, *inter alia*, moving the selected data to another processing system, for example for archiving purposes, or making the selected data unavailable. In automated filing systems the restriction of processing should in principle be ensured by technical means."

Unlike the GDPR, the LED contains a right to restriction of processing separate from the right of erasure.[90] Recitals 47 and 48 are explicit: Member states must create a right to restrict processing in national legislation, as a corollary to the right of erasure, and as a standalone right for data subjects. Article 16(3) LED mandates the restriction of processing where the accuracy of the personal data is contested by the data subject and the accuracy or inaccuracy cannot be ascertained or the personal data must be maintained for the purposes of evidence. Statements by victims and witnesses containing personal data are based on the subjective perceptions of the person making the statement. These statements are not always verifiable and are subject to challenge during the legal process. In such cases, the requirement for accuracy does not apply to the content of the statement but simply that a specific statement has been made. Furthermore, a statement may contain both facts and opinions, but sometimes may have to be categorised in either one of those categories, because the document

[87] Smolla, R. Law of Defamation, 2nd Edition, Thomson Reuters Legal, 2014.
[88] Custers B.H.M. (2018), Profiling as Inferred data: Amplifier Effects and Positive Feedback Loops. In: Bayamlioglu E., Baraliuc I., Janssens L., Hildebrandt M. (Eds.) *Being Profiled: Cogitas ergo Sum*. Amsterdam:
[89] Custers, B.H.M. (2003) *Effects of Unreliable Group Profiling by Means of Data Mining*. In: G. Grieser, Y. Tanaka and A. Yamamoto (eds.) *Lecture Notes in Artificial Intelligence, Proceedings of the 6th International Conference on Discovery Science (DS 2003)* Sapporo, Japan. Heidelberg: Springer, Vol. 2843, p. 290-295.
[90] Article 18 GDPR.

cannot be split into separate data items. It is unclear from the text of the Directive how law enforcement officials can then undertake the determination of whether a statement is fact or fiction.

4. Conclusions

While in some respects the LED brings data controller obligations for law enforcement authorities into the 21st Century, the LED contains conceptual issues and, in comparison to the GDPR, contains limited transparency requirements, lower thresholds for consent, and, in some areas, lower standards for protecting data subject rights. This paper identified three major conceptual issues. The first issue concerns the role of consent in the LED and the suggested empowerment and control that is offered to data subjects in the context of law enforcement. Although the LED uses consent as a central concept, in many ways similar to the GDPR, this is fundamentally at odds with the processing of personal data in a law enforcement context. The second issue is that the LED requires competent authorities to categorize data relating to witnesses, suspects, and victims. This is problematic, because a participant's role in a criminal event is both fluid and dynamic and the roles of data subjects typically change over time or sometimes even overlap. The LED approach to this fails to recognise these dynamics and complexities. The third issue is that the LED requires competent authorities to document whether data collected is a 'fact' or an 'opinion'. The problem here is that 'factual' accounts of witnesses and others are always inherently subjective. This is particularly relevant for inferred data, which may have error margins and may therefore not always be as facts. The LED´s requirement on competent authorities to categorize facts from opinions and to make a clear distinction between offenders, suspects, witnesses, and victims creates two categorisation quagmires. This puts recognized data protection principles of lawfulness, fairness, transparency in the crosshairs.

The suggestion that data subjects can actively influence who collects and processes their personal data and for which purposes via their data subject rights is misleading in a law enforcement context and suggests stronger forms of consent and higher levels of control than data subjects actually have. In practice, consent and control are hard to effectuate. The obligations to categorise data seem useful to keep the data in their context, but in practice these categorisations are also hard to apply. For all these concepts it can therefore be argued that they are hard to operationalise. When the goal is to offer better protection for data subjects, a focus on transparency and clear data processing limitations for data controllers may be more suitable than the suggestive concepts of consent and control that are hardly enforceable for data subjects. Less focus on data subject rights may seem counterintuitive when aiming for better protection, but may be more realistic from a practical perspective. When compensated with further regulation on transparency and clear data processing limitations, this may actually result in stronger protection of data subjects, as such regulation would always apply, whereas data subject rights only apply when actively invoked by data subjects.