DATA PROTECTION DIRECTIVE (EU) 2016/680 FOR POLICE AND CRIMINAL JUSTICE AUTHORITIES[1]

By Juraj Sajfert[+] and Teresa Quintel[*]

Literature

- Diana Alonso Blas, 'First pillar and third pillar: need for a common approach on data protection?' In: Gutwirth, S., Reinventing Data Protection? pp. 225–237. Springer, Berlin (2009).
- Diana Alonso Blas, 'Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom', ERA forum, August 2010, Volume 11, Issue 2, pp 233–250
- Franziska Boehm 'Information sharing and data protection in the Area of Freedom, Security and Justice – Towards harmonised data protection principles for EU-internal information exchange', Springer 2012;
- Lee A. Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', Computer Law & Security Review, 17.1 (2001), 17–24.
- Andrew Guthrie Ferguson 'The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement', in: New York University Press, 2017.
- Paul De Hert, Vagelis Papakonstantinou and Cornelia Riehle 'Data protection in the third pillar: cautious pessimism', in Martin Maik (Ed.), Crime, Rights and the EU: The Future of Police and Judicial Cooperation, London, Publisher: Justice, 2008, (196p.) 121-194;
- Paul De Hert and Vagelis Papakonstantinou, 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters — A modest achievement however not the improvement some have hoped for' (2009) 25 Computer Law & Security Review 403.
- 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 Juraj Sajfert, 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data' in Briere, C. and Weyembergh, A (eds), The needed balances in EU Criminal law: past, present and future, 2017, Hart Publishing.
- 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.
- Paul De Hert and Juraj Sajfert 'Police, privacy and data protection" in Monika den Boer (editor), 'Comparative policing", forthcoming.
- Linda E. Fisher, 'Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups', *Ariz. L. Rev.*, 46 (2004), 621.
- Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', *Digital Enlightenment Yearbook 2012* (IOS Press 2012).
- Gianclaudio Malgieri and Paul De Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably but Not Necessarily by Judges' in Gray, D. and Henderson, S. (eds), The Cambridge Handbook of Surveillance Law, Cambridge University Press, 2018.
- Thomas Marquenie 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', Computer Law & Security Review, 33 (2017), 324-340.
- Mario Martini, ‚DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling', in Boris P. Paal und Daniel Pauly (eds), *Datenschutz-Grundverordnung* (1st edn, beck-online 2017).
- 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.
- Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law*, 7.2 (2017), 76–99 <https://doi.org/10.1093/idpl/ipx005>.

Other references

- 'A further step towards comprehensive EU data protection', EDPS recommendations on the Directive for data protection in the police and justice sector'. Opinion 6/2015, 28 October 2015. (EDPS Opinion 6/2015)
- Article 29 Working Party, WP 251, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017. (WP29 Guidelines on Automated individual decision-making and Profiling)
- Article 29 Working Party, WP 258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 29 November 2017. (WP29 Opinion on some key issues of the Law Enforcement Directive)
- Eurojus, '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),'
Understanding and Preventing Discriminatory Ethnic Profiling: A Guide ; towards More Effective Policing, ed. by Europäische Union (Luxembourg: Office for Official Publ. of the Europ. Union, 2010).

[1] This article is a contribution to a GDPR commentary forthcoming in 2019 for Edward Elgar publishing.

[+] Official of the European Commission. The views expressed in this chapter are purely those of the author and may not in any circumstances be regarded as stating an official position of the European Commission.

[*] FNR funded PhD Candidate at the Université du Luxembourg and Uppsala University under the supervision of Prof. Mark D Cole and Assistant Prof. Maria Bergström.

I. Structure of the Directive

Processing of personal data by police and criminal justice authorities was, until recently, not an activity that caught a lot of attention of academia and practitioners[2]. Laws regulating such processing were perceived as dry, technical and fragmented[3]. Furthermore, these are not provisions concerning commercial activities generating income and affecting consumers of services, which was another reason reducing their attractiveness.

Although there is a lack of research covering regulations for the processing of personal data in the law enforcement sector, there is no doubt that such rules are rapidly gaining importance and visibility. There are at least three factors[4] contributing to the allure of previously neglected legal texts: firstly, an increased number of criminal acts is being committed online or with the help of online tools. Perpetrators of crime leave digital traces that may support law enforcement authorities (LEAs) in their tasks of crime prevention, investigation, detection and prosecution. Data collection and data exchanges progressively gained in importance for successful police work. Secondly, as perpetrators are becoming more tech-savvy, LEAs turned to new investigative techniques, including big data analytics. The term big data police technologies may include predictive systems that identify people or places suspected of crime, surveillance systems to monitor at-risk areas and search systems to mine data for investigative clues or to develop intelligence nets of helpful data for groups or across communities.[5] Thirdly, EU rules (both the patchwork of data protection rules adopted under the former third pillar[6] and the rules for EU Justice and Home Affairs Agencies[7]) on the processing of personal data by LEAs are undergoing consolidation, with Directive (EU) 2016/680[8] (LED) acting as a locomotive.

---

[2] However, very important work in this area was carried out by some academics in the past. In particular, see Franziska Boehm 'Information sharing and data protection in the Area of Freedom, Security and Justice – Towards harmonised data protection principles for EU-internal information exchange', Springer 2012; Paul de Hert, Vagelis Papakonstantinou and Cornelia Riehle 'Data protection in the third pillar: cautious pessimism', in Martin Maik (Editor), *Crime, Rights and the EU: The Future of Police and Judicial Cooperation*, London, Publisher: Justice, 2008, (196p.) 121-194; Diana Alonso Blas, First pillar and third pillar: need for a common approach on data protection? In: Gutwirth, S., 'Reinventing Data Protection?', pp. 225–237. Springer, Berlin (2009).

[3] See: 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 and 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.

[4] See: Paul de Hert and Juraj Sajfert 'Police, privacy and data protection from a comparative legal perspective" in Monica den Boer (editor), "Comparative policing', Edwar Elgar Publishing, forthcoming in 2018.

[5] Andrew Guthrie Ferguson 'The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement', NY: New York University Press, 2017, p.272.

[6] According to Article 62(6) of the LED, the instruments such as the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210/1 (6 August 2008), the Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210/12 (6 August 2008), or the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L386/89 (29 December 2006) should be aligned with the LED by 6 May 2019.

[7] See Chapter IX of the Regulation (EU) 2018/1725 of the European Parliament and of the Council 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, OJ L 295, 21.11.2018.

[8] 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 L 119, 4.5.2016, p. 89–131.

Like the GDPR, the LED was adopted in May 2016, constituting a major step forward in establishing a comprehensive EU data protection regime, as the first horizontal and legally binding instrument laying down the rules for national and cross-border processing of personal data in the area of law enforcement.[9] Moreover, the LED is a modern instrument, designed for LEAs processing personal data in the Digital Age.[10] As the second part of the data protection reform package that had been under discussion for four years, the Directive received way less attention than the GDPR. However, two main objectives of the Directive are too important to be neglected: the increased level of fundamental rights protection in the area of police and criminal justice, and the improved sharing of personal data between the Member States, as they will be able to rely on uniform data protection rules (Article 1(2)). The Directive is the successor to the 2008 Framework Decision 2008[11], which had a much more limited scope and solely applied to cross-border data processing between the Member States.[12] The rules of the Directive, which had to be transposed into the national laws of all 28 Member States and the four Schengen Area States (Norway, Iceland, Switzerland and Lichtenstein)[13] by May 2018 benefited from the attention given to the GDPR, as some of the Regulation's solutions could simply be taken over. However, a number of provisions were developed specifically for the Directive.

I.1. Meandering between the Directive and the GDPR

One of the most important provisions of the Directive is to be found at its very beginning. Article 1(1) defines the scope of the Directive, which is crucial for a clear delineation between the Directive and the GDPR. In order for the Directive to be applicable, both its personal and material scope have to be met. In other words, the processing must be carried out by a competent authority (personal scope) for the purposes of the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (material scope) (Articles 1(1) and 2(1) respectively). Whenever a police officer processes data for non-law enforcement purposes, for instance, and as the most obvious example, HR data or information that is to be archived, the GDPR will apply. Yet, in other areas where LEAs may be competent to process personal data, the delineation between the Directive and the GDPR is not as apparent. This might be the case in situations where police officers process personal data for identification or verification purposes in the field of migration and border control. A person crossing the Schengen borders irregularly might be checked by a police officer and, in those Member States where the irregular crossing of borders qualifies as a criminal offence, the police officer may change the purpose of the processing, depending on whether it is carried out for migration purposes or for prosecuting the criminal offence. However, once the irregular migrant applies for asylum, the processing of his application will fall within the scope of the GDPR, notwithstanding the initiated criminal proceedings. This demonstrates not only the complexity of the scoping exercise between the GDPR and the Directive,

[9] See: Thomas Marquenie 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', Computer Law & Security Review, 33 (2017), 324-340.
[10] Cf.: Paul de Hert and Juraj Sajfert 'Police, privacy and data protection from a comparative legal perspective', 2018.
[11] 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, OJ L 350, 30.12.2008, p. 60–71.
[12] On the shortcomings of the Framework Decision 2008/977/JHA, cf.: Paul De Hert and Vagelis Papakonstantinou, 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters — A modest achievement however not the improvement some have hoped for', (2009) 25 *Computer Law & Security Review* 403.
[13] The Directive is a development of provisions of the Schengen acquis. See recitals 101, 102 and 103.

but also the intricacy of competent authorities applying two different legal regimes, depending on the purpose of the processing.

I.2. Minor offences: a stumbling block of harmonisation

Several national legislators, in the exercise of transposing the LED, interpret its Recital (12) in a way that opens the possibility to include minor offences within the scope of the Directive. In other Member States, all types of offences are considered criminal offences and thus, trigger the applicability of the Directive in a general manner. Most of the Member States, however, will apply the Directive solely to *classic* criminal offences; consequently, in those Member States the GDPR will be applicable to minor offences. Such differentiated reading, also with regard to the determination of authorities that fall within Article 2(1) generally, and from what point they act as *genuine* LEAs that carry out processing for law enforcement purposes more specifically, leads to a fragmented delineation between the GDPR and the Directive across Member States, which is an undesirable result, as the reform's objective is the harmonization of data protection rules across the Union.

I.3. Blurred lines between law enforcement and national security

In accordance with the above, the Directive should apply only if both the personal and the material scope are satisfied. If one of the two criteria is not met, either the GDPR or other EU instruments[14] will apply, unless the processing is being performed for purposes falling completely out of scope of EU law, in which case none of the EU Regulations/Directives will be applicable (for example, when a military intelligence service is collecting data about persons plotting to threaten the national security of a country by destroying its crucial army bases). Although the legal basis of Article 16 TFEU, on which both the GDPR and the Directive were adopted, is very strong and not a lot of processing activities will fall outside the scope of EU law, the latter does not cover processing carried out by national intelligence and military agencies. This may become problematic where a clear delineation between the different tasks of intelligence agencies is lacking. Therefore, when national intelligence agencies process data for the purposes of the Directive, they should be viewed as competent authorities under Article 2(1) instead of not being covered by EU law. This issue becomes even more relevant in the context of information sharing between national intelligence agencies and LEAs.

I.4. *Croquis* of the Directive

The following section will briefly explain the structure of the Directive and underline both its differences and similarities with regard to the provisions of the GDPR.

The Directive, just like the GDPR, is divided in ten chapters. Three chapters, I (general provisions), IV (controller and processor) and VI (independent supervisory authorities) are closely linked to the GDPR, incorporating a number of the latter's provisions.

Chapter I reiterates a number of definitions from the GDPR and defines the scope of the Directive, which has been discussed above. It also explains that the Directive is not a full harmonisation instrument, allowing Member States to introduce higher data protection safeguards from the minimum standards required by the Directive.

[14] For instance, Regulation (EC) No 45/2001 if the processing is carried out by Union institutions, bodies, offices and agencies, or more specific legal regimes, such as the Europol Regulation (EU) 2016/794.

Chapter IV, just like the GDPR, introduces the risk-based approach and a number of new obligations for controllers and processors that resemble the ones stipulated in the GDPR (data protection by design and by default, DPIA, notifications of personal data breaches, obligation to appoint a DPO). The Chapter also establishes a duty to keep logs of certain processing operations (Article 25), which is a specific obligation under the Directive and a very important tool to monitor whether law enforcement databases are used lawfully. On that account, part II.3 of this contribution will devote more attention to this particular obligation.

Chapter VI lays down the same requirements as the GDPR regarding the independence of national supervisory authorities and the conditions for the appointment of its members. The Directive leaves it to the Member States whether they establish one supervisory authority competent for the application of both the GDPR and the Directive, or separate supervisory authorities that are responsible for either the Directive or the GDPR. Besides the restriction for the supervisory authorities to supervise courts acting in their judicial capacity (Article 45(2)), Member States may add further independent judicial authorities to be exempted from the administrative supervision of supervisory authorities when acting in their judicial capacity. The latter, optional exemption is designed for national authorities that maintain an equivalent level of independence to that of courts and judges[15].

Two chapters, VII (co-operation) and VIII (remedies, liability and penalties) endorse several provisions of the GDPR, while omitting the GDPR's provisions on the one-stop-shop, the consistency mechanism, provisions on the dispute resolution by the EDPB, joint operations of the supervisory authorities or the administrative fines under Article 83 of the GDPR. These notable omissions are due to the more basic structure of the Directive, resulting from the Council's anxiousness to keep the supervision of the police and criminal justice authorities within the exclusive remit of the respective national supervisory authority, without the meddling of a supervisory authority from one Member State into another Member State's police work.[16]

Three chapters: II (principles), III (rights of the data subject) and V (international transfers) strongly diverge from their equivalent provisions in the GDPR. They are specifically designed for the needs of LEAs and the particular nature of their processing activities. This is in line with the specificities of data processing by police and criminal justice authorities, recognised in Declaration 21[17] attached to the Treaty of Lisbon. On the other hand, those chapters may be perceived as weakening the overall level of protection given to data subjects in EU law and offering too much leeway to police and criminal justice authorities, compared to the remainder of the public sector covered by the GDPR.

In Chapter II, already at the level of principles of processing defined in Article 4 are some important differences compared to the GDPR. Firstly, the Directive does not refer to *further processing*, but instead introduces the notion of *subsequent processing* by the same or another controller in paragraphs 2 and 3. In the law enforcement context, such processing is generally deemed compatible with the purposes of the initial data collection (if the collection was also carried

[15] Cf.: Paul de Hert & Juraj Sajfert, 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data', in: Briere, C. and Weyembergh, A (eds), The needed balances in EU Criminal law: past, present and future, 2017, Hart Publishing, p.250.
[16] *Ibid*, p. 253.
[17] 'The Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.'

out for the purposes of the Directive), if authorized by law and if necessary and proportionate to the new purpose, to the extent that the new purpose remains within the scope of the Directive. Another notable difference is the principle of data minimisation (Article 4(1)(c)). Under the Directive, personal data should be *adequate, relevant and* ***not excessive****,* rather than *adequate, relevant and* ***limited to what is necessary,*** as stipulated under Article 5(1)(c) GDPR. Both principles grant more flexibility to LEAs in the performance of their tasks compared to the requirements of the corresponding provisions under the GDPR.

Furthermore, Article 6 introduces a specific obligation for controllers under the Directive to establish a clear distinction between personal data of different categories of data subjects (suspects, convicts, victims, witnesses). The LEAs therefore have to neatly tag and properly organise their databases, in line with the jurisprudence of the ECtHR[18]. Another principle specific to the Directive is laid down in Article 7, requiring personal data based on facts to be distinguished from personal data based on personal assessment. Additionally, 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.[19] As regards the basis for the lawfulness of processing, the Directive lays down only one legal ground in Article 8 (*if necessary for the performance of a task carried out by a competent authority for the purposes of the Directive and based on Union or Member State law*), while Article 6 of the GDPR provides for six different legal bases. Obviously, the legislator recognized that LEAs may only carry out tasks permitted by law, and not process data for the purposes of the Directive on the basis of consent, contractual obligations or the controller's legitimate interest.

Article 9 is another very specific provision of the Directive, with two different sets of rules. Firstly, paragraphs 1 and 2 provide the rules for interactions between the Directive and the GDPR. Secondly, paragraphs 3 and 4 authorise specific processing conditions to be attached to transmitted data. These conditions, however, may not be more stringent for the authorities of the receiving Member State than the conditions that are imposed on the authorities of the Member State transmitting the data.[20] With regard to the processing of special categories of data ('sensitive data'), Article 10 of the Directive, unlike Article 9 of the GDPR, does not establish a prohibition in principle. It allows the processing of sensitive data, but only where **strictly necessary** and subject to appropriate safeguards for the rights and freedoms of the data subjects. These are two important requirements added alongside the general lawfulness requirements pursuant to Article 8. Finally, Article 11 on automated individual decision-making was placed in Chapter II of the Directive instead of Chapter III, where one can find its GDPR equivalent. Apart from this organizational difference, the Article has some distinct features compared to Article 22 GDPR, which will be explained in part II.1. of this chapter.

Compared to the more 'generalist' Articles of Chapter III of the GDPR, the approach towards data subject rights and their possible limitations under Chapter III of the Directive is circumscribed in more detail, in order to adapt the means of processing personal data to the needs of LEAs. The basic set of rights remains the same (information, access, rectification, erasure, restriction of processing) and those rights may be exercised **directly** against the data controller. Understandably

[18] See ECtHR App nos 30562/04 and 30566/04 *S and Marper* v United Kingdom (4 December 2008)2008] .

[19] A good example of how this can be done in practice was developed in Article 29 of the Europol Regulation (EU) 2016/794 where different handling codes have to be attached to transmitted data, depending on the level of their reliability and accuracy.

[20] This is a police cooperation rule introduced in EU law by the so-called *Swedish Initiative* in 2006 - Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100.

the Directive does not provide for GDPR rights that were primarily designed to be exercised against commercial operators, such as the *right to be forgotten* or the right to data portability. The controller may limit the right of specific information to be given to the data subject, the right of access and the right to obtain information about the possible refusal of rectification, erasure or restriction of processing in a similar way as under Article 23 GDPR, i.e. if there is a legislative measure allowing for the limitation and if the limitation is necessary and proportionate. The grounds for such limitations are much narrower than under the GDPR and closely linked to the purposes of the Directive.[21] Given that the controllers may limit not only the rights, but also the information about the refusal to grant a certain right, a number of data subjects will receive a neutral reply. It is very difficult, or even impossible, to challenge such replies before courts, as data subjects will not be able to formulate what exactly they are referring to in potential complaints. This is why Article 17 provides for an independent review by the supervisory authority and the exercise of data subject rights indirectly, through the intermediary of the DPA. Article 17 will be further analysed in Part II.2 of this contribution. Finally, Article 18 allows Member States to lay down rules for the exercise of data subject rights in criminal proceedings in accordance with the provisions of the national criminal procedural laws. That means that the Directive is fully applicable to criminal proceedings, but since Member States' criminal procedural codes already provide for rules on information, access, rectification, erasure and restriction of processing, the provision recognises such codes as correct transposition efforts.

In Chapter V, which will be discussed in more detail in part II.4, international transfers shall be allowed, as a general rule, only from one LEA to another and after receiving the authorization of the originating Member State. For example, the French police may transfer personal data received from the German police to the FBI only after receiving the prior authorization of the German authority. As there are no comparable transfer conditions in the GDPR, the provisions on transfers under the Directive may be explained by the Council's and the European Parliament's desire to keep the original controller of operational law enforcement data in control over the use of such data by final recipients. The three-step architecture of conditions for international transfers (adequacy decision - appropriate safeguards - derogations) under the GDPR is replicated in the Directive, but the approach to data transfers by way of appropriate safeguards gives more flexibility to controllers, allowing them to carry out a self-assessment of such safeguards (Article 37(1)(b)). Finally, Article 39 is a very specific and novel provision providing for, as an exception from the rule, so-called *asymmetrical transfers* from a LEA in a Member State to private parties in third countries. This Article will be very useful for contacts between EU LEAs and service providers overseas, in particular in the fight against cybercrime and cyber-enabled crime.

Finally, chapters IX (implementing acts) and X (final provisions) contain usual and more technical provisions.

II. Four focal points of the Directive: profiling, indirect exercise of data subject rights, logs, international transfers

The second part of this Chapter will give an overview of four distinct features enshrined in the Directive. Due to the limitations in space and the primary purpose of this commentary to focus

[21] Articles 13(3), 15(3) and 16(4): Avoid obstructing official or legal inquiries, investigations or procedures; avoid prejudicing the prevention, detection, investigation, or prosecution of criminal offences or the execution of criminal penalties; protect public security; protect national security; protect the rights and freedoms of others.

on the GDPR, the selected provisions could only be discussed to a limited extent, albeit certainly meriting a more detailed analysis. The authors, therefore, decided to focus on provisions of the Directive that stand out for both their distinct nature and importance for practitioners. In line with the sequence of the Articles in the Directive, the discussion will first address automated individual decision making in Article 11, which might attract a lot of interest of LEAs in the context of new IT tools and other technical possibilities at their disposal. Furthermore, the chapter will focus on the indirect exercise of data subject rights under Article 17, which is a provision without an equivalent in the GDPR and also a game changer in improving data subject rights, compared to the current EU law provisions in the area of police cooperation and judicial cooperation in criminal matters. Our third ray of focus falls on Article 25 and the obligation for competent authorities to keep logs, which is another provision without a corresponding article in the GDPR and will require a substantive transposition effort from both the Member States and the LEAs.

Finally, the chapter will present the provisions on international transfers under the Directive, given these articles have a different logic than the ones under the GDPR and on the background that such transfers are becoming increasingly important in the international fight against cross-border crime.

II.1 Article 11

Automated individual decision-making

1. *Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.*

Despite extensively strengthened data subject rights under the Directive, specific provisions might not offer sufficient safeguards to protect these rights while responding to current needs and challenges for LEAs. In particular, trends to combine processing techniques, such as data mining, data matching and predictive analytics are often in conflict with fundamental data protection and privacy rights. These types of processing operations as well as different forms of profiling might be covered by different provisions[22] of the Directive, whereas Art. 11 is limited to decision-making *solely* based on automated means. Where processing involves (profiling-based) decision making that is not solely based on automated means, any '*preliminary profiling*' would not be covered under Art. 11 of the Directive.[23] For example, the Italian Lombardy region created a designated census of its Roma population.[24] If the purpose of this census would be to facilitate prosecution of crime committed by the members of that community, it could have constituted a form of ethnic profiling prohibited by Art. 11, but evidently, such census will not be carried out solely by automated means. Only once a created profile is subsequently processed by solely automated means, this will trigger the applicability of the provision.

[22] Articles 4 (principles relating to processing of personal data), Article 8 (lawfulness of processing), Article 10 (processing of special categories of personal data) and Articles 13 to 17 (information to be made available or given to the data subject, right of access by the data subject, limitations to the right of access, right to rectification or erasure of personal data and restriction of processing, and exercise of rights by the data subject and verification by the supervisory authority).

[23] WP29, 'Guidelines on Automated individual decision-making and Profiling', p. 23.

[24] Decision of the Lombardy Regional Council NOXI/40 of 3 July 2018, also reported about in La Stampa at http://www.lastampa.it/2018/07/04/esteri/lombardy-moves-forward-with-roma-census-DoA54EOBA3srT6LE3d1lVO/pagina.html, last accessed on 8 September 2018.

The wording of Art. 11 suggests that the Directive could, hypothetically, provide stronger data protection standards regarding automated processing than the GDPR. While the latter stipulates, in its Art. 22, that data subjects *'shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or* ***similarly significantly*** *affects him or her'*, Art. 11 of the Directive prohibits such processing if it '*produces an adverse legal effect concerning the data subject or* ***significantly*** *affects him or her'.* Thus, the Directive seems to provide more clarity regarding its terminology, referring to *any* significant effect caused by automated processing. While Art. 11 of the Directive clearly represents a prohibition, it could be argued that under Art. 22 GDPR, data subjects presumably have to assert their rights procedurally.[25] On the other hand, the WP29, in their Guidelines on automated individual decision-making and profiling,[26] suggest interpreting the provision of the GDPR as a prohibition.[27] Admittedly, there are strong arguments for interpreting Art. 22 GDPR as a right as well as a prohibition and those sets of arguments have to survive the test of time.

The GDPR is not limited to *adverse* legal effects, but includes all outcomes legally affecting data subjects as a result of automated decision-making processes.[28] However, it could be argued that Art. 22 GDPR kicks in only when data subjects are being affected by legal effects or **similarly significantly** affected by the outcome of the automated decision-making, while the language in the Directive is stronger and more straightforward, prohibiting automated decision-making when the data subject is **significantly affected,** without requiring a correlation with a legal effect.

II.1.1. Focus on the individual's rights: a potential loophole?

Neither Art. 11 nor the recitals of the Directive define what constitutes an *'adverse legal effect'*, according to Bygrave, however, legal effects '*alter or determine a person's legal rights or duties*' either partly or entirely.[29] Presumably, the Directive refers to results of automated processing that affect the legal status of a data subject by altering his or her legal rights *negatively*. On this account, it should also be mentioned that both the GDPR and the Directive merely prohibit *individual* decision-making. Consequently, collective or group profiling would not fall within the scope of Art. 11. However, competent authorities might create profiles of groups during border surveillance or police monitoring operations, despite the fact that such groups have a collective interest of protecting their privacy and enjoying the same data protection rights as those that are granted to individuals. Due to this current loophole in EU data protection law, the interests of these groups of individuals are not protected.[30]

'[…] *unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject* […]'

Reference to Recital 38 of the Directive suggests that '*appropriate safeguards*' consist of the provision of specific information to the data subject, including the right to obtain an

[25] Mario Martini, 'DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling', in: Boris P. Paal und Daniel Pauly (eds.), *Datenschutz-Grundverordnung* (1st edn, beck-online 2017). Rn 29.
[26] WP29, 'Guidelines on Automated individual decision-making and Profiling'.
[27] Ibid, p. 8.
[28] Mario Martini, ‚DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling',Rn 28; Martini questions whether the GDPR refers to *adverse* legal effects and mentions the German *Bundesdatenschutzgesetz*, which only includes negative legal effects and finds that the GDPR's wording is less clear in that regard.
[29] Lee A. Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', in: *Computer Law & Security Review*, 17.1 (2001), 17–24.
[30] Cf. Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics', in: Philos. Technol. (2017) 30: 475. https://doi.org/10.1007/s13347-017-0253-7.

explanation of a decision that has been taken concerning him or her subsequent to the automated processing operation. In addition, data subjects should, according to that recital, have the right to challenge such a decision. However, the non-binding nature of recitals, the legal nature of the Directive (depending on its transposition in the Member States), and its applicability in the law enforcement area (naturally leaving more discretion to the controller), indicate that such a right to information is not to be treated as being equivalent to the right enshrined in Article 15(h) GDPR, which provides for the right to obtain information of the existence of automated decision-making and the logic involved in such processing. However, under the Directive, data controllers shall provide data subjects with the information set out in Article 13, including, in specific cases, information concerning the legal basis of the processing, the data retention period and the categories of recipients of the personal data. The controllers will be obliged to provide such information customarily.

II.1.2. Understanding policing through mathematical models

The right to '*express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision*' as set out in Recital 38, however, is not explicitly contained in Art. 11. It could be argued that the text of the said recital is explaining the last part of Article 11(1), i.e. *'at least the right to obtain human intervention on the part of the controller'*. However, obtaining an explanation of a specific decision might prove difficult, due to the recital's non-binding character and because a majority of algorithms are protected by trade secrets or intellectual property rights.[31] Consequently, these restraints limit the possibility to challenge a decision that is based on automated decision-making.

The Directive, like the CJEU in its PNR Opinion 1/15[32], requires human intervention when processing of personal data is carried out solely by automated means. However, this obligation is only mandatory when a decision that might adversely affect the data subject is being taken. In other words, when automated processing was carried out, but no decision has been taken, the result of that processing operation could theoretically be used for *subsequent* processing.

The right to obtain human intervention on the part of the controller remains rather uncertain in the texts of both the GDPR and the LED. As the wording suggests that *any* human intervention in an automated decision-making process makes the latter no longer *solely automated*, that requirement is rather ambiguous.[33] Article 11 does neither require *human intervention* to be anything more than nominal, nor does it oblige a controller to verify and scrutinize the substance, rationale or final decision of an automated decision-making measure.[34] Would any nominal human intervention, regardless at what point during the processing, therefore allow data controllers to refrain from providing appropriate safeguards for the rights and freedoms of data subjects? The impact of Article 11 on clarifying the opacity of algorithms that decide what kind of action the police will take towards any given individual might therefore remain rather limited.

[31] Moreover, explaining the algorithms used for law enforcement purposes might provide insight in the strategies of competent authorities and could potentially jeopardize ongoing investigations. See also: Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', in: *International Data Privacy Law*, 7.2 (2017), 76–99 <https://doi.org/10.1093/idpl/ipx005>.
[32] Opinion 1/15, para. 141.
[33] Ibid. cf.: Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', *Digital Enlightenment Yearbook 2012* (IOS Press 2012). And Lee A. Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', (2001) 17 Computer Law & Security Review 17.
[34] Martini,(n 1). Rn 16-19.

2. *Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

The second paragraph of Article 11 resembles Article 22(4) GDPR, with the exception that the GDPR, in Article 9, prohibits processing based on special categories of data, unless, pursuant to paragraph 2(a) and (g) of that Article, certain conditions for derogating (allowing such processing based on the explicit consent of the data subject or processing for purposes of public security), are satisfied. A general prohibition to be contained also in the Directive was proposed by the EP after the first reading[35] and recommended by the EDPS[36], however, not maintained in the final text of the Directive. It is, therefore, essential to understand what the suitable safeguards required by the Directive in this provision are. Certain guidance is provided in Recital 37, which suggests, *inter alia,* the possibility to collect sensitive data only in connection with other data on the natural person concerned, to secure the data collected adequately, to implement stricter rules regarding the access to sensitive data by law enforcement staff, and a prohibition to transfer such data. In addition, the verification of data accuracy, the application of ethical guidelines and combining profiling based on sensitive data with traditional methods of investigation would be an imaginable tool to ensure the lawfulness of processing. For example, profiling individuals based solely on religious beliefs is prohibited. However, if an individual, for which there is a reasonable suspicion of involvement in terrorist activities, is a member of a religious group, it might be necessary to take automated decisions based on his or her personal data related to the worshipping place, religious preachers etc.

3. *Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.*

In return, Article 11(3) of the Directive stipulates an absolute prohibition of discriminatory profiling based on special categories of data[37], a provision that is non-existent in Article 22 of the GDPR. Thus, in order to be lawful, a profile may not consist of data *purely* relating to i.e. the race, ethnicity or religious affiliation of the data subject[38] if its use could lead to any discrimination of the data subject that would not be objectively and reasonably justified. The police should '[…] *carry out their tasks in a fair manner, guided in particular by the principles of impartiality and non-discrimination'*.[39] This provision under Article 11(3) is to be welcomed, as the risk of discriminatory and racial profiling seems to be particularly high in the context of data retention, predictive policing, surveillance[40] and the technological developments regarding such methods.[41]

[35] Article 8, 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; P7_TA(2014)0219.

[36] 'A further step towards comprehensive EU data protection', EDPS recommendations on the Directive for data protection in the police and justice sector'; EDPS Opinion 6/2015,, p.7.

[37] Which was not included in the COM proposal from 2012, but first in the EP's decision after the first reading (Article 9(2b)) from March 2014. See: European Parliament legislative resolution of 12 March 2014; P7_TA(2014)0219.

[38] *Understanding and Preventing Discriminatory Ethnic Profiling: A Guide ; towards More Effective Policing*, ed. by Europäische Union (Luxembourg: Office for Official Publ. of the Europ. Union, 2010). P. 20.

[39] Committee of Ministers of the Council of Europe, Recommendation Rec(2001)10 on the European Code of Police Ethics, 19 September 2001 and Explanatory Memorandum, available at: http://www.coe.int/t/cm/adoptedTexts_en.asp. Para. 40.

[40] Linda E. Fisher, 'Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups', *Ariz. L. Rev.*, 46 (2004), 621.

[41] However, even if such sensitive data are deleted during the data collection phase, the aggregation of 'non-sensitive' data may easily allow to draw conclusions about data subjects that reveal similar information.

Two requirements that apply to profiling measures under the GDPR and that would have been advisable to impose also when carrying out automated decision-making under the Directive are (1) the obligation to conduct a DPIA prior to such processing and (2) the right to obtain information concerning the consequences of automated processing as stipulated in Article 15(f) GDPR. Although representing a new obligation for data controllers introduced under the Directive, a DPIA needs not to be carried out for the sake of profiling, as is particularly the case under Article 35(3)(a) of the GDPR. However, Article 27 of the Directive requires that, whenever the processing (in particular when using new technologies) is likely to result in a high risk for individuals, a DPIA needs to be carried out in order to mitigate data protection risks as good as possible.[42] This requirement will become very relevant regarding the use of new technologies for data mining techniques, predictive analysis and profiling by competent authorities.[43]

In the area of law enforcement, consequences following specific processing operations of personal data may be specifically pertinent for the data subjects concerned, particularly in the case of data breaches (Article 30(c)). That is why data breaches should be communicated to the data subject unless this would jeopardize ongoing investigations (Article 31(5)). In certain cases, such as for minor offences, obligatory notification by the controller or processor would be appropriate.

II. 2 Article 17

Exercise of rights by the data subject and verification by the supervisory authority

1. In the cases referred to in Article 13(3), Article 15(3) and Article 16(4) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.

The provisions of Chapter III of the Directive grant data subjects the right to address data controllers directly with their requests (for access and subsequent rectification, erasure and restriction of processing). Previously, the 2008 Framework Decision, in its Articles 17(1)(a) and 18(1) allowed Member States to *choose* whether they allow data subjects to either directly assert their rights against the controller or through the national supervisory authority as intermediary[44]. Similar deference to Member State rules is provided for under the data protection rules applicable to the Second-generation Schengen Information System (SIS II), in particular under Article 41 of the SIS II Regulation and Article 58 of the SIS II Decision[45].

[42] 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.

[43] Conversely, the WP29 recommends the national legislators to place an obligation on controllers to carry out a DPIA in connection with automated decisions. See WP29, 'Opinion on some key issues of the Law Enforcement Directive', p. 15.

[44] Cf.: Diana Alonso Blas, 'Ensuring effective data protection in the field of police and judicial activities', pp. 233–250.

[45] 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 and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the Second-generation Schengen Information System (SIS II), OJ L 205, 7.8.2007, p. 63–84. Although already in October 2014 the SIS II Supervision Coordination Group noted in its report on the exercise of the rights of the data subject in the Schengen Information System, only five Member States have the system of indirect access to personal data in SIS – France, Germany, Belgium, Luxembourg and Portugal, while France and Germany also have a direct access. In 2016, The Commission issued three proposals for: a Regulation on the establishment, operation and use of the Schengen Information System in the field of police cooperation and judicial cooperation in criminal matters, COM(2016) 883 final, a Regulation on the establishment, operation and use of the SIS in the field of border checks, COM(2016) 882 final, and a Regulation on the use of the SIS for the return of illegally staying third country nationals, COM(2016) 881 final, all Brussels, 21 December 2016. The Council and the European Parliament reached an agreement on the new texts in June 2018, and they should be formally adopted and published in the Official Journal by the end of the year.

II.2.1. Strengthening data subject rights – direct access as a rule

However, the Directive obliges controllers to accept direct requests of data subjects. In addition, it creates an obligation for Member States to provide for the indirect exercise of data subject rights through the intermediary of a supervisory authority, in cases where the controller has decided to limit the right of specific information to be given to the data subject (Art. 13(3)), the right to access (Art. 15(3)) and the right of information to the data subject about the refusal of his or her request for rectification, erasure of restriction of processing and concerning the reasons for such refusal (Art. 16(4)). All Member States will, therefore, have to oblige their LEAs to directly deal with data subjects' requests and to provide data subjects with the required information. Member States will also have to empower their supervisory authorities to indirectly exercise data subject rights in case a controller decides to limit them. This two-level approach to the exercise of data subject rights is a novelty for almost all Member States, who have so far chosen to provide for either the direct or the indirect exercise of data subject rights. The new approach, therefore, significantly improves the situation of data subjects whose data are being processed by LEAs, as it introduces another line of checks by an independent supervisory authority. As a consequence, the new approach of the Directive will have a spill-over effect on the EU databases such as SIS II, as the national rules referred to in the abovementioned SIS II instruments will become the national laws transposing the Directive.

II.2.2. Exercising data subject rights in three steps

The rationale behind this novel system lies in the necessary counterbalance to the three-step approach to the exercise of data subject rights under the Directive, which is at the same time different and more specific than the one of the GDPR. The first step is a simple situation in which the competent authority decides to fully grant data subject rights. In that scenario, the police will proactively inform a data suspect, in accordance with Article 13(2), that his or her data are being processed, communicate the legal basis for processing, disclose the applicable storage period etc. Most of the categories of data subjects should receive such information: victims, witnesses, experts, convicts, and even suspects in later stages of proceedings, when provision of such information would not jeopardise the investigation anymore. Upon request, the competent authority will also have to provide the data subject with access to his or her personal data being processed (Article 14) and eventually rectify inaccurate data held about him or her (Article 16(1)). The second step refers to a more complex situation, which requires a legislative measure allowing for a limitation and a necessity and proportionality assessment of such limitation, after which the competent authority will limit data subject rights. For instance, the competent authority will not provide information as to the origin of the personal data in order to protect the informant (Article 14(g) in conjunction with Article 15(1)). In such cases, the competent authority should inform the data subject about the refusal to provide information relating to the origin of the personal data in question and the reasons that led to the refusal.

However, in some cases, in particular when LEAs are dealing with speculative requests of data subjects, already providing information about the refusal to grant a certain right might present too much information. Sometimes the mere revelation that certain data are held in a police database might jeopardize ongoing investigations against a suspect. The Directive, therefore, envisages a third step, in which competent authorities may decide not to give any sort of information to the data subject and instead provide a neutral reply to his or her inquiry (Article 15(3) second sentence) - '*we can neither confirm nor deny your data is being processed'*. Such replies are frustrating for data subjects and leave them completely in the dark. Particularly during the second step, and even

more the third step, the role of the supervisory authorities under this Article is crucial in order to ensure that data subject rights are being fully respected.

2. Member States shall provide for the controller to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1

Article 12, which is a general provision of Chapter III, applicable to all subsequent provisions on data subject rights, provides in its paragraph 3 that competent authorities must inform the data subject in writing about the follow-up regarding his or her request without undue delay. Hence, competent authorities must rather quickly[46] reply to data subject requests. Depending on their assessment, competent authorities may grant full access, rectify or delete personal data (step 1), can limit fully or partially the request and provide an explanation as to the grounds for limitation (step 2) or they might give a neutral reply to the data subject (step 3). If they choose to limit the rights of the data subject in line with step 2 or 3, their reply should inform the data subject that he or she has the possibility to exercise his or her rights indirectly through the intermediary vested in the supervisory authority. This valuable information should secure that the possibility of an indirect exercise of data subject rights is actually used in practice.

3. Where the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

When data subject rights are being exercised indirectly, the supervisory authority will have to ensure that the competent authority lawfully processes personal data, that the data in question are accurate and complete, get rectified if inaccurate, deleted when processed unlawfully, etc. There are, therefore, a number of checks the supervisory authority needs to carry out before replying to the data subject's request. However, the replies of the supervisory authorities should also be drafted with outmost diligence. A supervisory authority should inform the data subject what checks have been carried out, without revealing the reasons which led the competent authority to the decision to limit the rights in the first place. In case the competent authority provides a neutral reply that is deemed justified by the supervisory authority, the latter will not be able to provide the data subject with details concerning the data processed or whether any data has been processed, apart from the fact that it has carried out all the necessary checks. The data subject should in any case be informed that, if still not satisfied, he or she is entitled to seek judicial remedy before a competent court.

The approach to the indirect exercise of data subject rights under Article 17, in particular, when the competent authority provided a neutral reply to the data subject who then faces a situation of not knowing which personal data are being kept about him or her, let alone whether they are accurate and processed lawfully, seems to be inspired by the relatively recent judgments of the ECtHR *Roman Zakharov v. Russia*[47] and *Szabò and Vissy v. Hungary*[48]. In both of these judgments, the ECtHR required proper and independent oversight of secret surveillance and the obligatory

[46] The WP29 Guidelines on the Directive suggest that the reply should be given within one calendar month after the receipt of a request. See Article 29 Working Party, WP 258, 'Opinion on some key issues of the Law Enforcement Directive', p. 19.
[47] ECtHR App no 47143/06 *Roman Zakharov v. Russia* (11 December 2015).
[48] ECtHR App no 37138/14 *Szabò and Vissy v. Hungary* (12 January 2016).

notification of the person under surveillance as soon such notification would no longer jeopardise the purpose of a surveillance measure.[49]

Extracting the basic requirement of the ECtHR and translating the two judgments it into 'data protection language', it seems that the independent oversight of the lawfulness of processing whenever data subject rights are restricted in a way that the data subject is prevented from obtaining information or access to data directly from the competent authorities is imperative. Article 17 of the Directive empowers supervisory authorities with such an independent oversight in addition to the effective investigative, corrective and advisory powers that supervisory authorities must be equipped with under Article 47. A small caveat in the end: the authors of this chapter are aware of the fact that supervisory authorities cannot act under Article 17 if the competent LEA limiting data subject rights is in fact a (criminal) court acting in its judicial capacity, given that the supervisory authorities do not have any competence over courts acting in their judicial capacity (Article 45(2)).

II.3 Article 25

Logging

1. Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

The obligation to keep logs of six processing operations in automated processing systems is a distinct feature of the Directive, without any equivalent provision in the GDPR. It is a much stronger obligation compared to the one under Article 10 of the 2008 Framework Decision, which, due to its purely cross-border nature, required logging or documentation only for **transmissions** of personal data. In EU law, the importance of logs is recognized in instruments such as the SIS II and the Visa Information System (VIS)[50], which focus on that issue in much more detail than the Framework Decision.[51] In the SIS II for instance, every access to and all exchanges of personal data within the central system have to be logged and these logs should be kept between one and three years, so that both the competent authorities internally and the independent supervisory authorities externally are able to verify whether searches in the database have been carried out

[49] Cf.: Gianclaudio Malgieri and Paul De Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges', in: Gray, D. and Henderson, S. (eds), The Cambridge Handbook of Surveillance Law, Cambridge University Press, 2018; Cole/Quintel, '"Is there anybody out there?" – Retention of Communications Data: Analysis of the status quo in light of the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), Carolina Academic Press Global Papers Series (forthcoming 2019).

[50] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ P. 120 – 141. In May 2018, the Commission issued a proposal for the revision of the VIS, see: Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 302 final, Brussels, 16.5.2018.

[51] For example, Article 12 of the SIS II Decision or Article 34 of the VIS Regulation, although in those texts logs are referred to as 'records'.

lawfully, by persons authorised to access the SIS II, and whether the reasons for access were justified.

This consolidation of the obligation to keep logs under the Directive as a comprehensive horizontal instrument, and its expansion compared to the Framework Decision is significant: from one processing operation (transmission) to six (collection, alteration, consultation, disclosure including transfers, combination and erasure); from a choice between logging or documenting to a standalone provision on logs, given that keeping documentation (records) is already stipulated in Article 24 of the Directive; and the applicability of the provision to all automated processing systems, which practically means that all law enforcement databases must be in compliance with the obligation to keep logs. As law enforcement databases contain high volumes of information on a large number of individuals, a lot of which are sensitive data, the logs play a central role in ensuring that such databases are not being abused and are only accessed by persons with proper authorization and with valid reasons to access retained data.

Out of six processing operations covered by this provision, the Directive gives particular importance to two processes: **consultation** and **disclosure**. These are the most common and also the riskiest processing activities in databases, which is why the Directive provides a lot of detail on the exact content of such logs. Firstly, these logs should identify the person who consults the database or who discloses the information from the database to a third party.[52] Secondly, in case of disclosure, the recipients of personal data should be identified as well. Thirdly, the exact date and time of the consultation or disclosure must be recorded as the basic feature of logs. Fourthly and most intriguingly, a hitherto unprecedented requirement to be included in logs is the **justification** for performing a processing operation. When reading a log, it must be possible to conclude why a certain officer consulted a database or disclosed data to a third party. The justification may be demonstrated in different ways, depending on the nature of the database, its technical features and the user profile. Sometimes it will be sufficient to identify the user and understand why a certain database was consulted (as Recital 57 suggests). In other cases, databases will have to include a drop-down menu or a free field where the user will record the justification for consulting it.

Due to all of the new abovementioned logging requirements, the implementation of this provision might prove to be costly and/or technically difficult, in particular for older automated processing systems. The Directive, therefore, allows, under Articles 63(2) and (3), for a longer transposition period of Article 25(1), for databases set up before the entry into force of the Directive, i.e. prior to 6 May 2016. Exceptionally, Member States may take additional five or even eight years to transpose this provision by 2023 or 2026 respectively, if the transposition causes massive costs or jeopardizes the functioning of the database as such.

2. *The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.*

Competent authorities have to carefully comply with the provisions that lay down the rules on the keeping of logs and documenting the purposes for which they are kept. The logs reveal a lot of information concerning the work of law enforcement officers but also about persons whose personal data are being consulted. They should therefore be kept and used solely for the purposes known from the 2008 Framework Decision, the SIS II and the VIS rules (verification of lawfulness

[52] See in particular Rec. 57, second sentence.

of processing, self-monitoring, integrity and security of the personal data) and for one new purpose introduced by the Directive – for criminal proceedings.

Logs can nowadays be kept through a log collector and monitored by a dedicated team within the competent authority through random checks of the log files and pre-defined automatic alerts, in order to discover potential misuses of information. It is possible to programme the alerts so that they notify the person responsible about any unusual or unauthorised operation in a database. The self-monitoring also includes disciplinary proceedings against law enforcement officers breaking or bending the rules, such as the ones abusing their access rights in order to check personal data of celebrities or random cars parked in front of their girlfriends' houses. If properly kept and monitored, logs are a powerful tool to prevent law enforcement officers from grave personal data breaches, such as the one recently discovered within Europol, where an employee took home and leaked an entire database online[53]. Moreover, logs may also be used in criminal proceedings as e.g. evidence in criminal proceedings against law enforcement officers selling police data on the DarkNet. But, they could also be used in criminal proceedings against a perpetrator of another type of a crime. For example, by matching logs of consultation of a border control database, conclusions can be reached about movements of a suspect. However, logs are above all safeguards and should not lead to further interferences with the right to privacy and data protection. The WP29, therefore, suggest a narrower reading of Article 25(2) where the use of logs in criminal proceedings would be adequate only when the lawfulness of a data processing operation is being challenged, when there is a security breach in dispute, or if the integrity of data is at stake.[54]

3. *The controller and the processor shall make the logs available to the supervisory authority on request.*

Ultimately, it will be up to the supervisory authorities to breathe life into the obligation of competent authorities to keep logs. Relying solely on self-monitoring would prevent the full exercise of different investigative of corrective powers of the supervisory authorities. It is crucial that the competent authorities keep logs for a certain period of time, ideally not less than two years[55], in order to allow for enough time for regular checks by supervisory authorities. They need to confirm whether self-monitoring is being done properly and if suspicious behaviour of law enforcement officers is being investigated and sanctioned internally. The supervisory authorities should, therefore, regularly carry out random checks of logs and use their corrective powers against competent authorities who do not properly monitor and sanction the staff abusing their respective access rights to law enforcement databases.

II.4 CHAPTER V

Transfers of personal data to third countries or international organisations

Articles 35-39 of Directive 2016/680

Transfers by EU LEAs to third countries must satisfy the conditions for international transfers laid down in Chapter V of the LED. Due to the different level of data protection standards within the EU versus other parts of the world, Articles 35 to 38 stipulate additional restrictions to processing operations, applicable when personal data are leaving the Union. The articles in Chapter V are divided into **General Conditions** for international transfers, transfers on the basis of

[53] See: http://www.nu.nl/binnenland/4357991/terrorismedossiers-straat-groot-veiligheidslek-europol.html.
[54] See: WP29, 'Opinion on some key issues of the Law Enforcement Directive', p. 27.
[55] On this issue, the WP29 suggests a case-by-case approach and a differentiation between access logs and the logs on the history of data. See: WP29, 'Opinion on some key issues of the Law Enforcement Directive', pp. 27 and 28.

Adequacy Decisions adopted by the Commission, transfers subject to **Appropriate Safeguards**, and **Derogations** from the general conditions for transfers in specific situations. Article 39 lays down the conditions for so-called ***Asymmetrical Transfers***, that take place from LEAs in the EU Member States to private entities established in third countries.

II.4.1. Structure of international transfers under the Directive

Under the Directive, the logic applied to international transfers differs from the one applied under the GDPR, however, the architecture of Chapter V in both instruments is the same.

Apart from the requirement for international transfers to be based on an adequacy decision by the Commission, which is adopted along the same procedure as an adequacy decision under the GDPR[56], the general principles for international transfers, set out in Article 35 of the Directive, are different from the ones stipulated under the GDPR. First, such transfers must be necessary 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. Second, and as a general rule, international data transfers may only take place via official channels, hence, from one LEA in the EU to another LEA in the third country receiving the data. This provision in the Directive is similar to Article 13 of its predecessor, the 2008 Framework Decision, but, other than under the Framework Decision, and as an important novelty, is subject to certain derogations that will be elaborated below.

II.4.2. The originating Member State behind the steering wheel of international transfers

Where a Member State transfers data that were obtained from another Member State, the latter must, pursuant to Article 35(1)(c), authorize such an international transfer before it may be executed. This procedure can, in situations of an immediate threat to public security, be accelerated and may, pursuant to paragraph 2, take place without prior authorisation.

Onward transfers of personal data by third country authorities must be authorised by the competent authority of the Member State from which the transfer originated[57]. For example, if a French authority would transfer personal data to an US authority, the latter would solely be allowed to further transfer such data to a Brazilian authority after the French authority authorised such an onward transfer.

II.4.3. The three-step cascade system

As mentioned above, the conditions for adequacy decisions adopted by the Commission for international transfers are equivalent to the ones under the GDPR[58]. Thus, it will be for the Commission to decide whether a third country ensures an adequate level of protection for personal data within the scope of the Directive. According to Recital 67[59] of the Directive, a third country

[56] An adequacy decision under the Directive is also a condition for international transfers by Europol to authorities of third countries, pursuant to Article 25 (1)(a) of Regulation (EU) 2016/794 of 11 May 2016. Likewise, according to Rec. 71, controllers, when assessing circumstances surrounding international transfers not based on an adequacy decision, should take into account cooperation agreements between Europol and Eurojust concluded with third countries.

[57] Taking into account *inter alia*, the seriousness of a crime, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organization to which personal data are onward transferred. Compare with the EU-US Umbrella Agreement, Art. 7.

[58] According to Rec. 68, relevant adequacy decisions adopted under Article 45 GDPR should be taken into account when assessing the level of protection in third countries for the purpose of international transfers under the Police Directive.

[59] Recital (104) of the GDPR.

should generally be able to provide a level of data protection that is '*essentially equivalent to that ensured within the Union*', as further required by the CJEU in its *Schrems*[60] judgment.

In the absence of the aforesaid decision, and in order to allow for more flexibility, the second step in the cascade are international transfers subject to appropriate safeguards. Article 37 foresees two situations in which such appropriate safeguards may exist, thereby departing from the similarities with, and being less specific than Article 46 of the GDPR. In the first option any appropriate safeguard shall be guaranteed in a legally binding and enforceable instrument, to provide administrative or judicial redress to the data subject concerned. A typical example of an instrument created to become this first option in accordance with Article 37 is the EU-US Umbrella Agreement.[61] Another option provided for by Article 37 is a decision to transfer data based on a self-assessment evaluation carried out by the controller. In such a case, the controller must evaluate the circumstances of the transfer with regard to the existing data protection standards in the recipient state, must inform the supervisory authority of the categories of data included in such transfer and document the transfer for potential review by the supervisory authority.

The final step of the cascade is Article 38, under which the Directive allows Member States, in certain situations, to derogate from the conditions under Articles 36 and 37. Derogations are only permitted in individual cases and solely if they serve to protect the interests of the data subject, if they are instrumental for the prevention of an immediate threat, or the establishment, exercise or defence of legal claims. Where the fundamental rights and freedoms of the data subject prevail over the public interest, international transfers on the basis of Article 38 may not take place.

II.4.4. A novelty – asymmetrical transfers

As the most innovative provision of Chapter V, the Directive, under Article 39, provides the data protection framework for data requests from LEAs in EU Member States directly to private parties in third countries. Since the procedures for requests via official channels may be very lengthy[62], such *asymmetrical transfers* anticipate the prevention of obstacles and smoother, direct cooperation with third country service providers. For that purpose, Article 39 imposes a number of conditions on the competent authorities in the Member States for data requests addressed to service providers in third countries, thereby derogating, in individual and specific cases, from the requirements in Article 35 to use the official channels only.

However, in order for Article 39 to apply, all other conditions of the Directive need to be satisfied. The legal basis for such transfers must be laid down in Union or Member State law (Article 8) and an adequacy decision under Article 36, appropriate safeguards pursuant to Article 37, or an individual derogation from Article 38 must exist, in line with the cascade described above. In addition, transfers under Article 39 must be **strictly necessary** for the investigation of a particular criminal offence; thus, fishing expeditions or bulk transfers are not permitted. This requirement calls for a strong link between the main tasks of the transferring authority and the necessity to transfer personal data. The fundamental rights and freedoms of the data subject may not override the public interest for the purpose(s) of which the transfer is carried out and the service providers must be informed about the purpose(s) for which the transferred data may be processed.

[60] CJEU C-362/14, *Maximilian Schrems*, ECLI:EU:C:2015:650.
[61] 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 L 336, 10.12.2016, p. 3–13.
[62] In the fight against cyber-crime, LEAs in the European Union will often perceive the mutual legal assistance channels as being too slow and will have to establish a direct contact with a service provider in a third country (e.g. Microsoft, Apple, Yahoo, Google, Facebook, Twitter etc).

Furthermore, a direct transfer to service providers may only take place if the competent authority in the State of the establishment of the recipient is not trustworthy or overwhelmed with requests, meaning that data exchanges cannot be carried out in a timely manner via the official channels. The third country authority should nevertheless be informed of the transfer, but again, if the authority is corrupt or unavailable (i.e. in a failed state) or simply prefers not to be notified, the competent authority in the transferring Member State does not have to comply with this requirement.

II.4.5. Stronger role for the supervisory authorities

The strict legal framework under which derogations for *asymmetrical transfers* may occur is monitored by the (vigilant) eyes of the supervisory authorities in the EU Member States. They must be informed whenever transfers under Article 39 of the Directive are carried out and have the power to *ex post* review documented transfers. The national supervisory authorities are therefore required to invest much more resources and to approach their respective police and criminal justice authorities with greater authority, compared to the situation before the entry into force of the LED.

II.4.6. International data exchange agreements with third countries

Because data processing in the field of judicial cooperation in criminal matters and police cooperation was, until recently, mainly left outside the scope of EU law, a vast majority of EU Member States concluded bilateral or multilateral agreements for the transmission and exchange of personal data to and with third countries.[63] Since Article 39 is without prejudice to these international agreements in force between the Member States and third countries, such agreements could, in theory, allow less strict standards for *asymmetrical transfers* than those required under the Directive. However, no such agreements are currently in force[64], and, as part of the EU *acquis*, the Directive prevents Member States from entering into international agreements that could dissolve the exceptional character of *asymmetrical transfers* and loosen the conditions stipulated in Article 39. Thus, if, in the future, Member States enter into international agreements on the exchange of data held by private parties, the data protection conditions laid down under these agreements may not be weaker than the ones pursuant to Article 39. When contacting service providers in third countries, LEAs in Member States will therefore have to show compliance with the data protection standards under the LED.

II.4.7. The particularities of international transfers in the area of law enforcement

The LED aims at balancing the flexibility needed for carrying out transfers to third countries for the purposes set out in Article 1(1) with the data protection rights of the individuals concerned. While such flexibility is required for the investigation of criminal offences and the safeguarding of public security, when personal data move across borders this may put at increased risk the ability of natural persons to exercise their data protection rights and to protect themselves from the unlawful use or disclosure of their personal data.[65] Oversight powers by supervisory

[63] Eurojus '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)', p.7.

[64] The first international agreement explicitly allowing for direct cooperation between EU LEAs and the service providers in a third country, and vice versa, is the UK-US agreement currently being negotiated. See more at https://www.hatch.senate.gov/public/index.cfm/releases?ID=D82974EA-BA0C-494B-A3A1-89A7926FB802.
Also, in April 2017 Google asked for a new approach to cross-border access to electronical evidence. See https://www.blog.google/topics/public-policy/international-framework-digital-evidence/.

[65] Rec. 74 of Directive 2016/680.

authorities within the Member States will be much reduced once the data has left the European Union. This is particularly true for onward transfers by third countries and international transfers that are carried out without establishing their basis on an adequacy decision. The execution of international transfers requires close overview by the Member States' supervisory authorities, strict interpretation of derogations and *ex post* review of documented transfers in order to protect data subjects' fundamental rights.

While the Directive certainly contributes to a less fragmented general framework for international transfers, it cannot cover all the fields in which transfers of data might take place. Pursuant to Article 2(3)(a) of the Directive and as mentioned previously, transfers of personal data between authorities responsible for safeguarding national security will not be covered by the provisions, as these generally fall outside the scope of the Directive. This may particularly become problematic in Member States where intelligence agencies and LEAs form part of the same organizational structure and data are commonly exchanged between these authorities.[66]

III. Conclusion

Article 16 of the TFEU conferred very broad competences to the Union to legislate on data protection matters. On the basis of this provision, it would have been possible to establish a uniform data protection regime applicable to all processing operations of personal data falling within the scope of EU law. However, one size does not fit all, and the co-legislators, therefore, opted for a separate legal instrument, the Directive for police and criminal justice authorities. The LED adopts some of the GDPR's solutions, but also has many standalone, distinct features. The Directive is undoubtedly a major step forward[67] compared to the data protection rules the EU had established under its third pillar (Justice and Home Affairs) prior to the entry into force of the Lisbon Treaty.

The Directive contains a comprehensive and forward-looking set of rules, receptive towards law enforcement activities in the Digital Age. This was demonstrated on the examples of principles (purpose limitation and data minimisation) that are more flexible than the equivalent provisions under the GDPR. The same holds true for some of the novel features introduced by the Directive, such as the use of logs for criminal proceedings, the possibility for competent authorities to carry out a self-assessment of appropriate safeguards surrounding international transfers, or the derogation allowing international transfers directly to private parties in third countries.

At the same time, the LED empowers data subjects with a strong set of rights and offers a higher level of protection. This chapter presented the additional safeguards on which data subjects may rely, for instance, against automated individual decision-making. Moreover, the mechanism for independent oversight by competent authorities through the supervisory authorities and the indirect exercise of data subject rights were illustrated and the detailed rules on the obligation for competent authorities to keep logs of the processing activities in law enforcement databases, as one of many new obligations of the competent authorities under the Directive were explained. Finally, the chapter laid down the conditions that must be followed when transfers of personal data to third countries are carried out.

[66] For instance, in Lithuania, Poland or Sweden.

[67] See Paul de Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive', p. 17 and Thomas Marquenie 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', Computer Law & Security Review, 33 (2017), 324-340.

In the context of the ongoing '*privacy v security'* discussion, the Directive shows that it now will be possible to achieve high privacy and data protection standards while processing personal data for law enforcement purposes in a more flexible manner. It would, therefore, be instrumental to shift the public debate from the false paradigm that either one or the other may be achieved. Today, the LED presents a benchmark for the consolidation and alignment of other EU data protection rules in the area of police cooperation and judicial cooperation with its rules (Article 62(6))[68]. Despite all, the effectiveness of the Directive will largely depend on its transposition within the legal system of each individual Member State. The general applicability of the Directive and the wide discretion of national legislators as to achieving the instrument's objectives might lead to considerable variations among the Member States, as was the case with the implementation of, for instance, Article 15 of the DPD.[69] In particular, there are risks of an overly broad interpretation of the scope of the Directive, at the expense of the GDPR. This situation is generated by the ambiguous language of Article 1(1) of the Directive and its accompanying Recital 12. They seem to broaden the applicability of the Directive from the core criminal law enforcement realm to the 'safeguarding against and the prevention of threats to public security' when certain police actions, such as undertaken during the major sporting events, riots or demonstrations may or may not lead to a criminal offence. Moreover, despite Recital 13 of the Directive, the latter left the notion of 'criminal offence' completely undefined, thereby making it entirely dependent on the interpretation of that notion under national law. The powers of supervisory authorities are yet another area where the transposition might turn out to be fragile, while the full potential of the Directive can be achieved only through a strong enforcement of its rules by these authorities. This is another weakness of the Directive, concretely its Article 47. Unlike the GDPR, which is very explicit on the powers of the supervisory authorities in its Article 58, the Directive does not oblige the Member States to vest their national supervisory authorities with any particular corrective powers in respect of police and criminal justice authorities, rather providing a few examples under Article 47(2) and introducing a general requirement that such powers need to be effective. In any event, there are no valid reasons to undermine the full transposition of the Directive, given that '*the police should follow what is in the Directive anyway*'.[70]

[68] By May 2019, the Commission has to propose the alignment of regimes such as Prüm (Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1–11 and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 12–72) or the Swedish Initiative (Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100). Moreover, the rules of the Directive have been taken over for some EU agencies active in this area. See in particular the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, p. 1–71.

[70] Valsamis Mitsilegas, scholar of European Criminal Law at Queen Mary University of London, during the House of Lords EU Committee session on Brexit and EU data protection, 17 July 2017.