Report

This part of the EDPL hosts reports in which our correspondents keep readers abreast of various national data protection developments in Europe, as well as on the most recent questions in different privacy policy areas. The Reports are organised in cooperation with the Institute of European Media Law (EMR) in Saarbrücken (www.emr-sb.de) of which the Reports Editor Mark D. Cole is Director for Academic Affairs. If you are interested in contributing or would like to comment, please contact him at mark.cole@uni.lu.

European Union

Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive

*Teresa Quintel**

I. Introduction

On 29 November 2017, the Article 29 Data Protection Working Party (WP29) adopted its 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)'[1]. The Law Enforcement Directive (LED)[2], which is a *lex specialis* to the more prominent General Data Protection Regulation 2016/679 (GDPR)[3], will have to be transposed into national legislation by 6 May 2018. It thereby repeals Framework Decision 2008/977/JHA[4] that is applicable to cross-border processing of personal data by competent law enforcement authorities. The scope of the LED is much broader than the one of the Framework Decision, as the Directive is applicable for all types of processing by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences whereas the Framework Decision was limited to the specific category of cross-border processing. In addition, the Directive strengthens the rights of data subjects and provides for new obligations imposed on controllers. However, since the Directive will leave a certain margin of discretion to the Member States when transposing it, and because the 28 criminal justice systems are not harmonised, the application of its scope may differ, due to the varying definitions of criminal offences or competent authorities, and the different competences provided to the latter.

Several provisions in the LED leave room for interpretation by national legislators, which could hamper the harmonisation of data protection standards in the area of law enforcement. Against this background, the WP29 Opinion of November 2017, emphasize several key issues of the LED, particularly focussing on the role of Data Protection Authorities (DPAs), data subject rights, obligations for controllers and aspects where the Directive might leave room for Member States to transpose the LED in a different manner than anticipated. The guidance provided by the WP29 addresses Article 5 (time limits for storage and review), Article 10 (processing of special categories of personal data), Article 11 (auto-

* Teresa Quintel, FNR funded PhD Candidate at the University of Luxembourg and Uppsala University under the supervision of Prof Mark D Cole and Assistant Prof Maria Bergström. For correspondence: <teresa.quintel@uni.lu>.

1 Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (29 November 2017) <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178> accessed 2 March 2018 (WP29 Opinion).

2 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 119/89.

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

4 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 350/60.

mated individual decision making and profiling), Articles 13 to 17 (rights of the data subject), Article 25 (logging) and Article 47 (powers of the data protection authorities) of the LED. In doing so, it seeks to encourage a consistent interpretation of key definitions, to prompt national legislators to further determine certain elements in their national laws and to clarify both the role of controllers in granting data subjects rights as well as the powers of DPAs to effectively control the enforcement of these rights.

II. Points of Concern Mentioned in the Opinion

1. Overview

On the whole, both assessment and recommendations regarding the key issues of the LED presented by the WP29 Opinion endorse an approach that is favourable towards high data protection standards. The Working Party calls on national legislators to foresee the implementation of coherent rules and to further define provisions in domains where uncertainties remain. Particularly with regard to data subject rights and effective powers of national DPAs, the WP29 seeks to set clear limits on the margin of discretion that national legislators might use to grant controllers more flexibility when processing personal data within the scope of the LED, as will be shown in more detail below. The WP29 proposes clear rules on retention periods (Article 5) and provides guidance on how to implement the logging requirement under Article 25.

Regarding Article 10, the WP29 suggests several measures that are to be welcomed, for instance, the performance of a Data Protection Impact Assessment (DPIA), or the prior consultation of the national DPA when processing special categories of data.

Concerning the recommendations on automated individual decision-making and profiling under Article 11, the Opinion seems rather vague with regard to certain aspects where the WP29 does not further clarify the scope of human intervention and omits guidance on how to effectively enforce the rights mentioned under Recital (38) in practice. Nevertheless, the Opinion endorses surprisingly strong safeguards for data subjects and urges controllers to carry out a DPIA in connection with automated decisions.

To ensure the effectiveness of Articles 13 to 17, the WP29 suggests interpreting the provisions in favour of strong data subject rights, enforceable obligations for controllers and seeks to set limits to possible limitations under Article 13(3) and (4) and Article 15.

With regard to Article 47, the WP29 urges Member States to foresee effective and enforceable powers for national supervisory authorities and to combine the monitoring of both Directive and GDPR under the competence of one single DPA in order to ensure consistent data protection standards.

It is, however, regrettable that the WP29 neither discusses the scope of the LED in comparison to the GDPR nor goes into detail concerning the transfer of personal data to third countries further than within the context of effective powers of supervisory authorities.

2. Article 5 on Time-Limits for Storage and Review

The guidance provided by the WP29 concerning time limits for storage and review for the erasure of personal data, and in particular the recommendation to introduce a mixed system that includes both maximum retention periods and regular review of the necessity for storage, should certainly be taken into account by national legislators. Where the Directive allows for more flexibility and leaves Member States the choice to introduce either time limits *or* periodic review, the WP29 proposes a much stricter approach. Here, the Working Party endorses a transparent assessment of the need for continued retention[5], procedural measures to ensure a data quality review with the involvement of the Data Protection Officer (DPO) and comprehensible documentation of procedural measures that is to be provided to the DPA.[6]

Adjusting storage periods along different types of crimes and carrying out a risk assessment where data is retained for preventive purposes should be applied as an expedient tool to determine the least intrusive measure and to ensure fair processing.

---

5 The WP29 underlines that where data stored for preventive purposes are to be retained for a prolonged period, such decision should always be accompanied by a risk assessment of the respective data subject and include the same safeguards as the ones regarding continued retention mentioned above. Such assessment is not to be confused with a DPIA.

6 WP29 Opinion (n 1) 4.

The introduction of technical measures for the automatic deletion or anonymisation of personal data after the maximum storage period would ensure that data are not subsequently processed for purposes incompatible with the initial purpose for processing and would be in line with the data protection by design principle under Article 20 and the storage limitation principle pursuant to Article 4(1)(e). In order to ensure effective deletion and erasure after the maximum storage period, the WP29 recommends making statistical information on deletion and erasure available to both DPO and DPA on request and advises controllers to define, jointly with their DPO, related procedural measures.[7] These suggestions are important in order to ensure that Member States implement the technical and procedural measures to guarantee compliance with necessary retention periods.

3. Article 10 on Processing of Special Categories of Personal Data

It is to be welcomed that the WP29 suggests a DPIA and, by reference to Recital 37, the provision of additional safeguards for the processing of special categories of data, since the processing of such data always bears high risks for the rights and freedoms of data subjects, particularly in the area covered by the Directive. Accordingly, the WP29 recognizes that the processing of special categories of data within the context of the LED might lead to even higher risks than within the scope of the GDPR, although the Directive, contrary to the GDPR, does not generally prohibit the processing of special categories of personal data.

The WP emphasises the interrelation between Article 10 and Article 8 (lawfulness of processing) of the Directive and thereby clarifies the somewhat misleading wording of Article 10. Limiting the possibilities to process special categories of data to certain types of crime or to only allow their processing in cases of urgency seems very reasonable. This option should be reinforced by prior judicial authorisation, stricter technical measures, particularly high security standards, and additional access authorisation requirements, as suggested by the WP29.[8]

Moreover, the WP29 stresses that where voluntary agreement[9] by the data subject is used as *additional* safeguard to process special categories of data, the data subject must be informed in a clear and unambiguous manner by the controller and, with reference to Article 7(3) GDPR, be able to withdraw his or her agreement at any time.[10] Although it is to be welcomed that the WP29 requires that data subjects should be able to withdraw their voluntary agreement for the processing of special categories of personal data at any time, this could be misleading, as voluntary agreement can never present a legal basis under the Directive and the controller may nevertheless decide to continue processing these data based on the other applicable reason for processing. Still, any withdrawal of such voluntary agreement might lead to a re-assessment of the respective processing operation and could, for instance, lead to a decision in favour of less intrusive measures.

4. Article 11 on Automated Individual Decision-Making

With regard to the clarifications on Article 11, the WP29 greatly focuses on profiling, although the provision principally addresses automated individual decision-making and solely includes profiling where the latter is part of such automated processing.

Besides giving several examples for 'adverse' legal effects and 'significantly affecting the data subject', the WP29 does not assess the provision in depth: the Working Party neither clearly defines the scope of human intervention, nor enters into a discussion concerning situations in which no decision is being taken after automated processing measures.

In that regard, it is regrettable that the Opinion does not provide further guidance as to the moment where human intervention can be seen as 'true intervention' and whether it should always be required *ex ante* in a pre-assessment of the automated processing system via a DPIA, or *ex post*, after a decision was taken and is contested by the data subject.

On the other hand, the WP29 goes rather far when suggesting to grant data subjects similar rights as the ones under the GDPR and when determining how human involvement should be carried out. It is in-

7 WP29 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) 4.

8 ibid 8.

9 In the context of the LED, consent as safeguard is called 'voluntary agreement' in order to not confuse it with consent as a legal basis under the GDPR.

10 ibid 9.

deed very commendable that the WP29 requires human intervention to be *significant* and to be performed by a person who is able to understand the decision-making process and to explain the result to the data subject. Whether it is realistic to require controllers to provide for someone who is proficient enough to understand the underlying algorithms and who has the capacity to change the decision taken concerning a data subject, is debatable. Moreover, in practice this standard would probably be difficult to implement, as in automated systems, the algorithms are often protected by intellectual property rights. In that regard, the WP29 could have given further clarification as to what should be included in the explanation to be given to the data subject.[11] It might be exaggerated to assume that data subjects will be provided with an extensive explanation, the possibility to express their point of view on specific results and to challenge the decision in all cases, also because these options are solely mentioned in the (non-binding) recitals of the LED. Especially where profiling is carried out for preventive purposes, the scope of Articles 13(3)(b) and 15(1)(b) as limitations to the right of access and information and Recital 12[12] might be underestimated in that regard.

The connection of Article 27 with Article 13(2)(d) and the advice to carry out a DPIA prior to processing operations under Article 11 could increase the transparency and thus, accountability of automated decisions. The same applies for the prior consultation of the national DPA where decisions are based solely on automated processing. The question of whether these options could count as human intervention remains open.

It would be useful to clarify the transparency requirements where no decision was taken after automated processing took place and where results of the automated processing operations are used for further decision-making under Article 11. Such use could exacerbate the effects on the data subject and would, within a strict interpretation of Article 11, not require human intervention unless processing is carried out for decision-making purposes. Here, further clarification could be derived from Article 16(2), which requires the erasure of personal data where data was obtained from processing which infringes the principle of fairness relating to the processing of personal data under Articles 4 LED.

Finally, the wording on the prohibition of discriminatory profiling where such processing is based on special categories of personal data is (not only in the WP29 Opinion) deficient, as the creation of profiles resulting in discrimination on the basis of any type of data is prohibited. This wording is misleading under the LED and should have been further clarified by the WP29.

5. Articles 13 to 17 on Rights of the Data Subject

With regard to the right to information enshrined in Article 13 LED, the WP29 point to the difference between 'making available' and 'give' information to the data subject, which is crucial when considering general processing operations and processing that affects particular individuals. Such differentiation obliges controllers to make general information publicly available under Article 13(1) and to give specific information to data subjects in certain cases defined by law under Article 13(2).[13]

The WP29 extensively addresses the right to rectification or erasure of personal data and the right to restrict processing under Article 16, thereby emphasising that the list to claim erasure under Article 16(2) should be regarded as being non-exhaustive and data subjects should be able to request the erasure of their personal data in additional situations.

The WP29 sets strict requirements for the limitations of data subject rights, repeatedly reminds national legislators that the rights under Articles 13, 14, 16 and 17 may only be restricted in exceptional cases, and that controllers must always provide data subjects with adequate information concerning limitations as well as the additional possibilities to have their rights exercised indirectly *or* to lodge a complaint with the DPA. In that regard, a listing obligation of processing operations and situations in which

11 On this issue of the right to explanation under the GDPR, cf: 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' (2017) 7(2) International Data Privacy Law 76–99.

12 The wording of the Recital is: '[A]ctivities carried out by the police or other law-enforcement authorities also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence'.

13 29WP Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) 17.

controllers would not be able to decline the right to erasure or rectification would reinforce accountability towards the data subject. Moreover, the introduction of an autonomous right to the restriction of processing would strengthen the means of data subjects where the accuracy or completeness of data is contested.

The new possibility for data subjects to exercise their rights indirectly through the DPA is a further step to make controllers accountable towards data subjects and should be foreseen as stand-alone provision in national legislation. However, the WP29 recommendation for controllers and supervisory authorities to document indirect access requests in registers in order to keep track of them and for statistical purposes remains rather unclear, as the WP29 neither specifies whether these registers shall include personal data, nor how long such registers should be kept.[14]

6. Article 25 on Logging

The WP29 considers the logging requirement under Article 25 to be crucial on the one hand to prevent unauthorised access or use of personal data and, on the other, to serve as means to prosecute any abusive use of data. Pursuant to the data protection by design principle, any automated processing system should customarily require the creation of logs whenever data is being processed within the scope of the LED.[15] To that end, the WP29 recommends that every person consulting personal data processed in an automated processing system should automatically be subject to the logging obligation, irrespective of whether the individual is *directly* involved in processing the personal data for the purposes of Article 1(1) LED, or needs to access the data eg for the purpose of system maintenance.[16]

Since Article 25 LED does not lay down further requirements regarding the content of logs or their storage periods, the requirement to specify these elements under national law, preferably on a case-by-case basis, is imperative. For that objective, the WP29 recommends an alignment of retention periods with the purposes of the respective logs and, where necessary, to consider the archiving of logs. Thus, a log that serves self-monitoring purposes on access might require shorter retention periods than logs that were created for the investigation of criminal proceedings. In addition, the WP29 acknowledges that in certain situations logs might have to be kept for longer periods, as may be the case for processing for preventive purposes. In any event, storage periods should give supervisory authorities sufficient time for review in accordance with Article 25(3).

With regard to the use of logs for criminal proceedings, the WP29 recalls that the purposes of logs, eg the verification of the lawfulness of processing, self-monitoring purposes, or ensuring the integrity and security of the personal data, must be the underlying basis for the use of logs in criminal proceedings.[17] Consequently, logs may solely be used in order to investigate unlawful processing, to monitor processing by staff and to prosecute unauthorized access or other data and security breaches, as any use going beyond these purposes would be excessive.

Finally, national legislation should define the technical measures, procedures for self-auditing and internal policies that will be required for an appropriate use of logs.[18]

7. Article 47 on Powers of the Supervisory Authorities

With regard to Article 47 LED, the WP29 acknowledges that, unlike the GDPR, the Directive does not provide for a detailed definition of the investigative, corrective and advisory powers of supervisory authorities. In order for them to be effective and enforceable, the WP29 suggests granting DPAs similar powers as the ones under the GDPR to ensure a comparable level of protection.[19] The WP29 further points to the necessity that all powers granted to the DPAs must be equally strong and binding, as otherwise their effectiveness would be insufficient.[20] In

14 ibid 24.

15 ibid 26.

16 ibid 25.

17 ibid 27.

18 ibid 26.

19 WP29 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) 30.

20 In the view of the WP29, a lack of corrective powers cannot be compensated by foreseeing the power to bring infringements to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings, as required by art 47(5). Such legal proceedings are supposed to be additional instruments and not alternative instruments to effective corrective powers. WP29 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) 30.

order to increase their independence, it makes sense to provide DPAs with strong powers under both GDPR and the Directive to avoid tensions between operational requirements and acceptable data protection standards.[21]

Moreover, the WP29 suggests, in accordance with the financial capabilities and constitutional structure of the Member States, to establish one DPA to monitor the application of both the Directive and the GDPR, instead of entrusting two separate authorities for the monitoring of each instrument.[22] One single supervisory authority for both GDPR and LED could contribute to a more consistent interpretation of the rules and lead to a coherent approach regarding data protection policies and practices.

III. Conclusion

21 Paul De Hert and Juraj Sajfert, 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data' in Chloé Brière and Anne Weyembergh (eds), *The needed balances in EU Criminal Law: past present and future* (Hart Publishing 2017) 243-255.

22 WP29 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) 30.