ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 258

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

Adopted on 29 November 2017

Introduction

The new Directive EU 2016/680 (Law Enforcement Directive – LED) complements the new Regulation EU 2016/679 (General Data Protection Regulation – GDPR).

The Directive is to be transposed by 6 May 2018 and oversees: 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. With the entry into effect of the Directive, the Council Framework Decision 2008/977/JHA (Data Protection Framework Decision - DPFD), which by 27 November 2010, Member States were required to implement, will be repealed. The decision applies to the areas of judicial cooperation in criminal matters and police cooperation, but, differently from the Directive, it is limited to the processing of personal data transmitted or made available between Member States and the further processing of such data as regards as well transfers to competent authorities in third Countries.

In order to suggest a coherent understanding and approach and due to varying stages of implementation and discussions within the Member States, the WP29 decided to focus on some key issues in its guidance, where practical guidance is needed or where these key issues directly concern the work of the Data Protection Authorities (DPAs) or where the course of implementation in one or more Member States suggests that the transposition may not be fully in line with the principles of the Directive.

Following this approach, the WP29 wishes to provide guidance by recommendations and remarks on the following articles:
Article 5 – Time limits for storage and review,
Article 10 – Processing special categories of personal data,
Article 11 – Automated individual decision making and profiling,
Article 13-17 – Rights of the data subject,
Article 25 – Logging,
Article 47 – Powers of data protection authorities.

At the same time the WP29 wishes to stress, that this is not an exclusive list and further guidance may be given in future if needed.

Article 5
Time limits for storage and review

Key topics
1. Maximum storage limits and periodic reviews
2. Distinctive time frames
3. Data protection by design

1. Maximum storage limits and periodic reviews

Where the processing of personal data within the scope of this Directive is carried out on the basis of Member State law, this should specify – along with the objectives and the personal data to be processed as well as the purposes of the processing[1] – the time-limits of each kind of processing.

Article 5 LED leaves it open to national legislators to provide for either appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. In any case, procedural measures shall ensure that those time limits are observed.

The WP29 considers that this wording leaves open the possibility to put in place a sort of mixed system allowing the combination of general maximum time limits with the periodical review of the need to keep for a further period the data stored in a way that allow the identification or the identifiability of the concerned individual (data subject).This is the best way to ensure full compliance with the principles relating to processing of personal data laid down in Article 4 LED ruling that personal data should be adequate, relevant and not excessive in relation to the purposes for which they were collected; personal data must also be accurate and, where necessary, kept up to date and in a form allowing identification of data subjects for no longer than is necessary for the purposes for which they are processed.

In this perspective, in principle, personal data should be processed until they serve the purpose for which they were collected and when they are no longer necessary for that purpose, they should be deleted, unless subsequent processing is foreseen by law and is deemed relevant for a purpose which is not incompatible with the original purpose for processing[2]. Alternatively, the Directive (and the GDPR) allow for retention in a form that does not allow identifying the data subjects. Both options should be considered.

[1] See Recital 33 LED and Art. 8.2 LED.
[2] In this perspective, see Article 4.3 LED which specifies that "processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects". Furthermore, in relation to the purpose limitation principle, see Article 9 LED whereby "Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1)

The question whether certain data have served their purpose and are no longer necessary, arises particularly when data storage is allowed for preventive purposes. It is inherent to such purposes that the storage can only be based on a risk assessment concerning a certain data subject. In such cases there is no point of closure, unlike in a criminal investigation, which automatically calls for a decision on deletion of the personal data collected during the investigation. Nevertheless, the principle of necessity calls for a review of the prognosis after an adequate time period. The decision to keep the data for another period should be well-grounded and the reasoning should be documented to make the review decision comprehensible.
Where time limits for the erasure of personal data in specific datasets are not directly established according to national law, the Directive foresees that a periodic review of the need for the storage should be carried out.

National law should provide for clear and transparent criteria for the assessment of the necessity to further keep personal data (such as the need to take into account updates related to judicial decisions or in case of rehabilitation of convicted persons, etc.), as well as for procedural requirements, so that the data quality principles are effectively met in order to avoid any abuse. To this end, whenever such a periodic review is carried out, the WP29 supports the involvement of the data protection officer (DPO) in the application of such criteria - inter alia with a view to a possible internal audit - and information on any decision to further retain the data and the reasons behind it, should be kept and made available to the relevant supervisory authority[3].

In a similar way DPOs must be involved in the definition of the procedure in order to effectively delete / erase the data once the time limits for the storage have expired.

WP29 considers it to be a good practice, as well as a tool for monitoring compliance, that statistical information on the deletion of data and the review procedure is made available both to the DPO and to the DPA, if requested.

unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law."

[3] For example, the Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol) lays down that Europol shall in any event review the need for continued storage and may decide on it if it is still necessary for the performance of Europol's tasks. The reasons for the continued storage shall be justified and recorded. If no decision is taken, data should be erased. Where the time-limits exceed the one settled by the provision, the competent Supervisory Authority (in this case, the EDPS) shall be informed accordingly (Article 31).

2. Distinctive time frames

When establishing maximum storage periods and periodic reviews, Member States should take into account the necessity and proportionality principles as interpreted by the European Court of Human Rights and the European Court of Justice[4].

Member States should make a distinction between categories of data based on their effective contribution for the purposes pursued and must use objective criteria for the determination of the length of the maximum storage period or periodic review.
For example, where relevant in the light of the case at issue the type or gravity of the underlying offence or risk has to be taken into account.

In addition, Article 5 LED must be read in connection with Article 6 LED, which calls for distinctions between different categories of data subjects (victims, suspects, persons convicted of a criminal offence, witnesses, experts, other persons involved). The obligatory distinctions must lead to a gradual regime of different timeframes to be envisaged in relation to the different categories of data subjects. Special attention has to be given to the protection of minors in this context as well. Existing and future databases have to be (re-)organized in a way that allows for the necessary distinctions to be made between different categories of data subjects.

3. Data protection by design

Within the context of data storage periods, the principle of data protection by design should be specifically implemented to promote compliance of data quality principles, in particular in alerting for the need to perform a periodical review and in automatically deleting data whose maximum storage period has already expired.

In this perspective, the maximum time-limits as well as periodic reviews foreseen by national law should be implemented via a well-structured IT-system based on "data protection by design".

Existing and future databases should be (re-)organized in a way that ensures periodic reviews to take place systematically as well as automatic deletion of data after reaching the maximum storage period.

In case of maximum time-limits, the system should ensure that the data are automatically deleted or anonymised as soon as the deadline for data storage has been

[4] As for an excursus on the application of these two principles within the law enforcement sector, see WP 29 Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, WP 211, 27 February 2014 and, more in general, for a useful "toolkit" to assess necessity and proportionality of a legal measure, see European data Protection Supervisor (EDPS), Assessing the necessity of measures that limit the fundamental right to the protection of personal data – A Toolkit, 11 April 2017.

reached. Pending the implementation of such a system, competent authorities should implement organisational measures in order to prevent any further use of these data.

In case of periodic reviews, the system should automatically remind the controller of the need to review the necessity of further processing. If the review is not done within a fixed period of time, the respective data should be automatically deleted or pseudonymised / masked.

In any case, taking into account the necessity and proportionality data protection principles, it could be envisaged that after a certain time, specific safeguards should be put in place in order to limit the access to personal data (for example, only authorised personnel could access those data for the purpose of specific operations within ongoing investigations and/or certain categories of data could be pseudonymised / masked).

Recommendations of the WP29

1. National laws on data processing within the scope of the Directive always should foresee maximum storage periods as well as periodic reviews of the necessity to keep the respective data. The review proceeding should be documented and the decision to extend the data storage period should be duly justified.

2. The principle of data protection by design should be specifically implemented within this context to promote compliance with the data quality principles. Existing and future databases should be (re-)organized in a way that ensures periodic reviews to take place automatically as well as automatic deletion of data after reaching the maximum storage period.

3. The assessment on the need to further store the data, as well as the establishment of maximum storage periods should reflect the different categories of data subjects

Article 10
Processing special categories of personal data

Key topics
1. Interrelation between Article 10 and Article 8 LED
2. Strict necessity
3. Appropriate safeguards
4. Voluntary agreement
5. Data manifestly made public by the data subject

1. Interrelation between Article 10 and Article 8 LED

Article 10 LED has to be read in connection with Article 8 LED. Therefore, the processing of special categories of data, if not foreseen by Union law, always requires a specific legal basis in national law (Article 10 (a)), as defined in Recital 33. This specific legal basis has to meet the additional requirements set up by Article 10 LED. Compared with Article 8 LED the processing has to be "strictly necessary" and "adequate safeguards" have to be set up.

The WP 29 recommends to interpret Article 10 (b) and (c) as merely illustrating specific situations, in which national law could foresee such processing. Article 10 (b) illustrates a situation, where vital interests of the respective data subject require the processing of special categories of data. Article 10 (c) illustrates a situation, in which the respective data subject itself has voluntarily relinquished the protection of the sensitive data by making them public.

2. Strict necessity

The differentiation between "necessary" (Article 8) and "strictly necessary" (Article 10) requires further interpretation, as it cannot be found in the case-law of the CJEU. In fact, it is settled case-law of the CJEU that any derogation or limitation to the protection of personal data must be "strictly necessary", as stated in the Digital Rights Ireland case: *"So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary."*[5]

[5] Digital Rights Ireland, CJEU, 8 April 2014, joined cases C-293-12 and C-594, § 52; see also Schrems, CJEU, 6 October 2015, C-362/14, §92; as for the use of a strict necessity test to assess legal measures, see also European Data Protection Supervisor (EDPS), Assessing the necessity of measures that limit the fundamental right to the protection of personal data – A Toolkit, 11 April 2017 and as for an excursus on the application of the necessity principle within the law enforcement sector more in general, see WP 29 Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, WP 211, 27 February 2014.

The WP29 concludes from this reasoning that the term "strictly necessary" in Article 10 has to be understood as a call to pay particular attention to the necessity principle in the context of processing special categories of data, as well as to foresee precise and particularly solid justifications for the processing of such data.[6]

To determine whether or not and to which extent the controllers may process sensitive data, a careful balance has to be found between the right to privacy and public interest. To this extent, the WP29 recommends, given the scope of application of the Directive and the sensitivity of the processing operations involved, that the competent authorities are committed to carrying out a data protection impact assessment (DPIA). It should be assessed and demonstrated whether the purpose of the processing (e.g. criminal investigation) cannot be achieved by processing which affects the rights and freedoms of the data subject less and if the processing of special categories of data does not represent a risk of discrimination for the data subject. Assessing the risk of abuse and discrimination, the foreseen safeguards have to be taken into account.

3. Appropriate safeguards

The processing of special categories of data always bears a risk that the data subject might suffer discrimination in violation of Article 21 of the Charter of Fundamental Rights of the European Union or other significant adverse effects to his or her rights and freedoms. The safeguards are appropriate if they are sufficient to protect the individual against those risks. A list of possible safeguards can be found in Recital 37.

Legal safeguards can be provided through additional material or procedural requirements. Additional material requirements could be additional limitations to the purpose of the processing (e.g. certain categories of crime), or in case of preventive measures a certain urgency (e.g. imminent danger with probably severe consequences for vital interests of many people). Recital 37 also mentions the possibility to collect those data only in connection with other data on the natural person concerned. Additional procedural safeguards could be the prior authorization of a court or another independent body and the prohibition of transmission of those data.

Legal safeguards should usually be accompanied/ implemented by technical and organisational measures like additional data security measures to ensure the confidentiality and integrity of the data and stricter rules on the access of staff of the competent authority to the data.

[6] For a similar approach taken by the CJEU in its opinion on the draft EU-Canada PNR-agreement, see Opinion 1/15, CJEU (Grand Chamber), 26 July 2017, § 141 and § 165.

4. Voluntary agreement

The consent of the data subject can never in itself constitute a legal ground for the processing of special categories of data in the context of the Directive. This is a major difference in comparison to the GDPR and this difference is stressed explicitly in Recital 35 which considers that Member States may provide by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive.[7]

In the light of this, the WP29 concludes that voluntary agreement should only be considered as an additional safeguard under the law in cases in which processing that is particularly intrusive to him or her are envisaged by law Therefore, it is for the national legislator to decide whether and to what extent to allow for data processing under the precondition of the data subject's voluntary agreement and whether to include special categories of data (see on this Recital 37[8]).

In such cases, the data subject should be informed in a clear and unambiguous manner by the competent authority about the voluntary nature of his/her agreement and should be given the possibility to withdraw it at any time (for example, in the case of collection of fingerprints or biological samples).

[7] Recital 35: *"The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law that the data subject may agree to the processing of his or her personal data for the purposes of this Directive."*

[8] *The latter is possible, as clarified in Recital 37, but must be explicit in the law: "The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities."*

5. Data manifestly made public by the data subject

According to Article 10 (c) national legislators may decide to allow the processing of special categories of data, if strictly necessary and guarded by adequate safeguards, for example, when those data have been manifestly made public by the data subject.

The WP29 wishes to emphasize that this has to be interpreted to imply that the data subject was aware that the respective data will be publicly available which means to everyone including authorities. In case of doubt, a narrow interpretation should be applied, as the assumption is that the data subject has voluntarily given up the special protection for sensitive data by making them available to the public including authorities.

In cases such as the publishing of personal data in a biography, in the press or on a public website the intention is clear. In other cases, this is more difficult to decide. For example, registering for a social network might include the acceptance of certain data protection rules which provide that all the partners of the provider (including national police authorities) have access to personal data. In such cases most of the users probably do not actively take notice of this and are in fact not aware that their data are available to police authorities.

Recommendation of the WP29

1. The processing of special categories of data, if not foreseen by Union law, always requires a specific legal basis in national law.

2. Article 10 calls for particular attention to the necessity principle regarding the processing of special categories of data, as well as to foresee precise and particularly solid justifications for the processing of such data.

3. The safeguards are appropriate if they are sufficient to protect the individual against the risk of discrimination or against significant adverse effects to the rights and freedoms of data subjects as prohibited by Article 21 of the Charter.

4. Within the scope of the Directive, voluntary agreement should only be considered as an additional safeguard under the law in cases in which processing that is particularly intrusive to the data subject are envisaged by law. Therefore it is for the national legislator to decide whether and to what extent to allow data processing under the precondition of the data subject's voluntary agreement and whether to include special categories of data.

5. Article 10 (c) implies that the data subject was aware that the respective data will be publicly available which means to everyone including authorities. In case of doubt, it should be interpreted narrowly.

Article 11
Automated individual decision making and profiling

Key topics
1. Definitions
2. Some key concepts of decisions based solely on automated processing, including profiling
3. Information obligations

Profiling and automated decision making are more and more developed in many sectors, including in the area covered by Directive.

Although they can be useful within the activities of competent authorities aimed to the specific purposes covered by Article 1, they can pose significant risks for individuals' rights and freedoms, and therefore require appropriate safeguards.

Similarly to the GDPR, the Directive specifically addresses "profiling" and "automated individual decision-making, including profiling".

With the Guidelines adopted on 3 October 2017, the Article 29 Working Party provided clarifications on the relevant provisions of the GDPR on automated individual decision-making and profiling and best practice recommendations. Such guidance is also relevant to Directive 2016/680, albeit with important caveats and some specifications.

1. Definitions

The LED defines "profiling" in Article 3(4) using a wording completely coincident with that used in the GDPR, thereby rendering applicable the considerations already expressed by the WP29 in the said Guidelines.

"Solely automated decision-making" refers to the ability to make decisions by technological means without human involvement in the decision process.

Although profiling and automated decision-making can be combined activities of the same process, they can also be carried out separately. There may be cases of automated decisions made with (or without) profiling and profiling which may take place without

making automated decisions. Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition.

2. Some key-concepts of decisions based solely on automated processing, including profiling

Solely automated individual decision

Article 11 sets out a general prohibition on "solely automated individual decision", including profiling, having an "adverse legal effect" or "significantly affecting" the data subject. The only exception to this prohibition is that such automated decision is authorized by Union law or a Member State law that provide suitable safeguards for the rights and freedoms of data subjects.9

Taking into account the specific nature of the processing carried out for law enforcement purposes, Article 11 LED does not contain any references to the other exceptions provided for Article 22 (2) of the GDPR, i.e.: (a) processing necessary for the performance of or entering into a contract; (b) processing based on the data subject's explicit consent. In this context, the WP29 would like to reiterate that consent could never work as the legal basis as there is a clear imbalance of powers between the data subject and the controller (such in this case).

Differently from the GDPR, the Directive provides that such prohibition applies to automated individual decision-making which produces not just a "legal effect" on the data subject, but an "adverse" legal effect. A typical adverse effect resulting from automated decisions could be the application of increased security measures or surveillance by the competent authorities.

However, the same Article considers that such prohibition is valid also in respect of a decision "significantly affecting" the individual such as for example in the case where a passenger is not allowed on board because registered in a black list, thereby expanding the scope of Article 11.

The adverb "significantly" excludes that trivial effects could be considered sufficient to enact the prohibition: the effect should be substantial enough to deserve attention and influence the individual.

[9] In this perspective the COUNCIL FRAMEWORK DECISION 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, repealed by Directive 680/2016, did not provide a definition on "profiling". However, Art. 7 regulated the automated individual decision stating that "A decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests".

Right to obtain human intervention

The Directive states that Member States' national legislator, when authorizing the decision based solely on automated processing under Article 11, must provide data subjects with the right to obtain human intervention on the part of the controller.
Although Article 11 only refers to the right to obtain human intervention and not "to express his or her point of view and to contest the decision" as provided for by Article 22 of the GDPR, it should be noted that according to Recital 38 of the Directive, in any case, such processing should be subject to suitable safeguards, including the "right to obtain human intervention, "in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision"".

As already underlined by the WP29 in its Guidelines on profiling, human intervention is a key element: it allows the data subject not to be submitted to indecipherable automated decisions which may suffer from errors or bias and allows him/her to have an exchange with the controller open to the additional elements or contestation the data subject may want to raise.

In this respect, it should be reiterated that, in order to be significant, the human intervention must be carried out by someone who has the appropriate authority and capability to change the decision and who will review all the relevant data including the additional elements provided by the data subject.

The prohibition against discrimination as a consequence of automated decision-making

Paragraph 2 of Article 11 sets forth the prohibition to base automated decisions on special categories of data (Article 10) unless suitable measures to safeguards the data subject's rights and freedoms and legitimate interests are implemented by Member States.

Due to the special nature of the data and the obvious risks of discrimination coming from automated decisions founded on such data, it is particularly important that Member States, while implementing the Directive, provide for strict safeguards for protecting individuals' rights.

The creation of profiles resulting in discrimination on the basis of special categories of data is prohibited per se by Article 11(3), in accordance with EU law.

Discrimination is unquestionably an example of a decision that significantly affects the data subject, and may entail adverse legal effects as well. Therefore Member States should consider that national law may not, under any circumstance, authorise profiling, that results in discrimination if based on the processing of sensitive data (Article 11.3),

whilst the automated decision making based on sensitive data is allowed, but only in the presence of a legal basis under EU or national law – which provides for the safeguards mentioned hereinafter (see Article 11(1) and (2))[10].

Data protection impact assessment

It should be recalled that the DPIA obligation under Article 27 (1) LED is worded identically to the corresponding provision in Article 35 (1) GDPR. Moreover, recitals 51 and 52 clarify, beyond any doubts, that profiling per se and even the mere processing of sensitive data as such entail risks to the rights and freedoms of data subjects, which may turn into a high risk under recital 52 if there is the particular likelihood of "prejudice to the rights and freedoms" of data subjects. Given the considerations made above on "adverse legal effects" that may be caused by automated decision making and on "discrimination" as an instance of automated decision making "significantly affecting" data subjects, the WP29 recommends to the national legislators to place an obligation on controllers to carry out a DPIA in connection with these processing operations. Such DPIAs may allow, in particular, identifying the specific safeguards and mitigations that have not been laid down in (more general) legislative measures enabling such automated decision-making; to that end, the preliminary consultation of the competent DPA as per Article 28 will play a key role.

3. Information obligations

In general, it should be recalled that the safeguards envisaged by Recital 38 should be provided by Member States' laws in accordance with Article 12 which clearly refers to the obligation for the controller to facilitate the exercise of the rights of the data subject under Articles 11 and the need for Member States to make sure that information on "any communication made or action taken pursuant to Articles 11 (…)" is provided "free of charge" (Article 12 (2) and 12(4)). Providing appropriate information, including as regards the existence of automated decision-making, including profiling, and meaningful information about the logic involved, to the data subject is particularly relevant also in respect of the fairness of the processing which should be ensured according to Article 4(1)(a).

As for the specific requirements related to the way and timing for providing transparency in relation to data processing carried out for law enforcement purposes, see paragraph 2 on data subjects rights of the present guidance.

Differently from the GDPR, the Directive does not explicitly indicate the need to include the existence of automated decision-making including profiling in the information to be

[10] See, for example, in this respect, Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Art. 6 (4) and Recital 15.

provided to the data subject under Article 13. However, due to the fact that automated decisions and profiling can be often "opaque" and be carried out without the data subject being aware, Article 13(2)(d) – which requires that "where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject, should be provided" - may apply subject to the provisions made in paragraph 3 of Article 13. These provisions are no different from those mentioned in Article 23(1), (a), (c), (d) and (i), of the GDPR, with the caveat that Member States "may" (under Article 13(4)) list the categories of processing subject to the restrictions mentioned in Article 13(3). The WP29 urges Member States intending to introduce such restrictions to provide the appropriate legal basis via legislative measures (see Article 11(1)).

Controllers should also be reminded that they are under the obligation to keep a registry of processing operations (pursuant to Article 24) specifying whether they carry out profiling. This is an important requirement, which is not envisaged in the GDPR in such a general manner and which MS should be especially vigilant in enforcing.

Recommendations of the WP29

1. The general prohibition on "solely automated individual decision", including profiling, having an "adverse legal effect" or "significantly affecting" the data subject should be respected. National laws providing exceptions to this prohibition under Article 11(1) must provide suitable safeguards for the rights and freedoms of data subjects, including the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision.

2. National law may not, under any circumstance, authorise profiling that results in discrimination if based on the processing of sensitive data (Article 11.3). Automated decision making based on sensitive data can be carried out only in the presence of a legal basis under EU or national law which provides for the safeguards mentioned hereinafter (see Article 11(1) and (2)).

3. National legislators are recommended to place an obligation on controllers to carry out a DPIA in connection with automated decisions.

4. Member States (without prejudice to the possible measures restricting the provision of information to the data subject according to Article 13(3)) must require the obligation of controllers to provide appropriate information to the data subject in particular where the personal data are collected without his/her knowledge (Article 13(2)(d)), which can be often the case when profiling and automated decisions are carried out.

Article 13 to 17
Rights of the data subject

Key topics
1. Rights of the data subject
2. Information to be made available to the data subject (Article 13)
3. Direct access as general rule (Article 14)
4. Restricted access (Article 15)
5. Right to rectification or erasure and restriction of processing (Article 16)
6. Indirect access (Article 17)

1. Rights of the data subject

First of all, it is important to see the interrelation of data subjects rights as described by Articles 13 to 17 of the Directive.

The articles provide for various cases where information should be provided and some exceptions. Article 13 LED describes an active obligation of controllers to provide certain information to data subjects. Some information has to be made publicly available (Article 13 (1)). More detailed information has to be given to a certain data subject in specific cases (Article 13 (2)). Exceptions to Article 13 (2) can be foreseen by law under certain conditions (Article 13 (3) and (4)).

Article 14 LED contains as a general rule the right of the data subject to access his personal data, which means the right to obtain directly from the controller positive or negative confirmation of the processing of his or her personal data (also known as the right of "direct access" by the data subject). In positive cases this includes the access to personal data and certain information.

Limitations to the right of direct access may be adopted by national law under the conditions laid down in Article 15 LED. In such cases the data subject usually has a right to be informed about the limitation and the possibility to lodge a complaint with the supervisory authority.

The transparency of data processing upheld by the right of access is not only a "right to know", but is further reinforced by the right for rectification, erasure or restriction of processing as laid down in Article 16 LED.

In case the law allows for limitations to the rights of information, access or rectification/ erasure, the data subject has a right of "indirect access" as laid down in Article 17 LED. In these cases, national legislation has to foresee the possibility to exercise the rights of information, access, or information about refusal of rectification or erasure by the

controller also through the competent supervisory authority at least. This right is to be distinguished from the right to lodge a complaint with the supervisory authority and constitutes an additional right in the framework of the Directive.

2. Information to be made available to the data subject (Article 13)

Making information available and being transparent with individuals about how their information will be used contributes to ensuring that the lawful processing of personal data is fair and controllers are themselves held accountable. Processing data under the scope of the Directive may sometimes be used in a manner that could cause some detriment to an individual. This is important because the processing of data under the Directive results in limitations on the individuals' freedoms and rights and is performed, at times, without the individuals being aware. Moreover providing information about the processing would assist with individuals' reasonable expectations.

Article 13(1) (a) to (e) defines the information the controller has to make available to data subjects. It should be noted that the wording of Article 13(1) refers to „making available" information, whilst Article 13(2) uses „giving" information „in specific cases". This would point to a difference in approach, whereby it can be argued that this duty does not relate to a certain data subject, but to a certain processing procedure and all data subjects potentially affected by it. Accordingly, this duty implies that the information has to be effectively made available in order to ensure that any data subject possibly concerned has been made aware of them.

In relation to Article 13(1), recital 42 provides examples as to how these pieces of information could be provided e.g. on the website of the competent authority. For example, a police force may wish to publish their privacy policy in relation to the use of custody images, Body Worn Video or firearms registration.

The pieces of information listed in Article 13(1) should always be made available. When giving the contact details of the DPO, the WP29 recommends that controllers also indicate that the DPO is one of the contact points for data subjects when addressing their requests. Article 13(1) (c) states that the purposes of processing should be included in the list of information provided. WP29 underlines that controllers should therefore be as transparent and as specific as possible about the law enforcement or policing purposes the data is being processed for.

Controllers should use techniques in whatever combination is most effective to present required information outlined to the data subject. The WP29 recommends to do so via the same medium used to collect personal information every time it is possible.

As explained above, while Article 13(1) is about general information made available to the public, 13(2) is about the information to be provided in addition to a particular data

subject in specific cases, for example where data is collected directly from the data subject or indirectly without the knowledge of the data subject.

Member States may adopt legislative measures delaying, restricting or omitting the provision of the information listed in Article 13(2) to the data subject to the extent that it is necessary and proportionate in order to avoid any of the prejudices outlined in Article 13(3). Any legislative measures must have due regard to the fundamental rights and the legitimate interests of the data subject.

The WP29 calls on national legislators to define objective criteria to determine in which cases and under which conditions the further information as outlined in Article 13(2) can be withheld by data controllers. Article 13(4) allows Member States to adopt legislative measures to determine which categories of processing may, either fully or partially, qualify under Article 13(3).

Articles 13(4) and 15(2) do not allow for blanket restrictions to data subject rights to information and access.

3. Direct access as a general rule (Article 14)

The Directive states that national legislators must provide for data subjects to have the right to obtain confirmation of processing and access to personal data being processed from the controller. This right is also specifically outlined in Article 8(2) of the Charter of Fundamental Rights of the European Union.

The WP29 underlines that there is a right of negative confirmation deriving from Article 14. A "neither confirm nor deny" policy is only possible in the case of derogations under Article 15.

Information should be provided free of charge without undue delay. The Directive does not define what 'without undue delay' means therefore the WP29 is of the view that controllers should provide information in response to a request under Article 14 to the data subject as soon as possible, where feasible within one month. Supervisory authorities should make a determination regarding compliance, where necessary, based on the representation and evidence provided by the controller and by the data subjects.

Domestic legislation must also ensure that the controller provides and communicates information to the data subject in a concise, intelligible and easily accessible form, using clear and plain language as per Article 12(1).

In addition, the list of information which needs to be included in a response to a right of access request includes information about the recipients or categories of recipients to whom the personal data has been disclosed. The Directive does clarify as to how specific the controller has to be in providing this information. The WP29 would like to remind national legislators and controllers of the essence of the right of access that is for the data subject to get a confirmation of the legal basis and be able to check the lawfulness of the processing. Therefore, controllers should make sure that the information provided is accurate, clear and sufficient to achieve this end.

In cases where the right of access is being fulfilled, WP29 would like to remind national legislators and controllers that Article 14(g) encompasses not only the origin of the data, but also all relevant information on how and under which circumstances the controller received them. It should also be remembered that data subjects have a legitimate interest in knowing where their data came from and, where possible, also the purposes for which the data were transmitted.

4. Limitations to the right of access (Article 15)

Article 15 provides for the only possibility for Member States to legislate to restrict, either fully or partially, the data subject's right of access as detailed in Article 14, as long as such a restriction constitutes a necessary and proportionate measure for the reasons listed in Article 15(1).

The WP29 would like to remind the national legislators that any exemptions from the fundamental rights and legitimate interests of the natural person should be applied as the exception rather than the rule and that omitting information may be allowed within an investigation only for as long as such a restriction constitutes a necessary and proportionate measure. The omitted information must, in accordance with the case law of the Court of Justice of the European Union, be provided once it is no longer liable to jeopardize the investigations being carried out[11].

Subject to Article 15, if data subject's right of access has been only partially limited and a response can be provided, the controller should provide access to the personal data being processed and the information listed in Article 14. If possible the information should be provided in the same form as the request. Whilst Article 14 does not explicitly state that the controller should provide a copy, where requested and possible, this should be provided in the context of an access request. Additionally, Recital 43 states that a summary of the data in possession of the controller could be provided.

If Member States opt to permit the ability for controllers to fully restrict the right of access to information outlined in Article 14, providing an exemption under Article 15 (1) can be applied, it is possible that no information would be communicated to the data subject. Therefore, the use of the concept of 'neither confirm nor deny' could be considered but again the WP29 would remind national legislators and controllers of the need to only apply an exemption where it is strictly necessary and proportionate, on a case by case basis, and that 'blanket' exemptions should not be used.

Even if the controller wishes to fully restrict the right of access, Member States must provide that the controller informs the data subject, without undue delay, in writing, confirming the refusal or restriction of access and the reasons. Again, as with Article 14 a response to the data subject should be provided within one calendar month of receipt of the request where feasible.

In response, controllers may omit the reasons for the refusal or restriction where an exemption under Article 15(1) is applied. Member States should ensure that controllers always provide an answer to a right of access request and that if the right of access is

[11] European Union Court of Justice, Opinion 1/15 of the Court (Grand Chamber) on the Draft PNR Agreement between Canada and the European Union, 26 July 2017; see, by analogy, judgment of 21 December 2016, Tele2 Sverige and Watson and Others, C 203/15 and C 698/15, EU:C:2016:970, paragraph 121 and the case-law cited.

being restricted or denied, the data subject is provided with information regarding the right to lodge a complaint with a supervisory authority and the contact details of this DPA or the option to seek a judicial remedy.

Additionally, under Article 15(4), where the right of access is restricted or refused, Members States must provide that controllers document the factual or legal reasons for that decision and such information must be made available to the supervisory authorities upon request.

5. Right to rectification or erasure and restriction of processing (Article 16)

Under Article 16(1), Member States shall provide for the right of data subjects to obtain rectification of inaccurate personal data relating to them, in particular when it relates to facts (recital 47), as well as, taking into account of the purposes of the processing, the right to have incomplete data completed, including by means of providing a supplementary statement. Controllers must ensure that they respond to these requests as soon as possible, where feasible within one month.

If inaccurate data is processed by controllers within the scope of the Directive, the possibility of this having adverse effects on individuals is high. Therefore, WP29 would like to remind national legislators and controllers of the necessity to ensure as far as possible that accurate data is processed and that founded requests to rectify data are processed with necessary urgency.

In relation to the erasure of data, Member States shall also, under Article 16(2), require controllers to erase personal data and to provide for the right of data subjects to obtain the erasure of personal data concerning them from the controller when the processing infringes the Directive (recital 47). The erasure of personal data is required where it was obtained from processing which infringes the principles relating to the processing of personal data, where it is unlawful, infringes the provisions of the Directive on the processing of special categories of personal data, or where personal data must be erased to comply with a legal obligation to which the controller is subject.

The list of processing which requires erasure under Article 16(2) should not be seen as exhaustive; national legislators and controllers should take into account the principal of the right as outlined in recital 47.

If, following a request to erase personal data, controllers determine that the personal data must be maintained for the purpose of evidence and where the accuracy of the personal data is contested by the data subject and the accuracy of that data cannot be determined, the Directive foresees the right to obtain the restriction of processing instead of erasure from the controller. This restriction may be undertaken via the technical means outlined in recital 47. In this case, the WP29 recommends that such

restrictions should be documented and mention for instance when the limitation started and stopped. In addition, the WP29 recommends that in case of a restriction of the processing the data should also not be sent to other controllers until the restriction is lifted.

The WP29 also underlines that even if the Directive does not expressly foresee a right to restriction in Article 16 separate from the right to erasure, as in Article 18 of the GDPR, recitals 47 and 48 of the Directive mention this right distinctly. Therefore, the WP29 encourages Member States to foresee the creation of such a right for data subjects in their national legislation, both as a corollary to the right of erasure and as a distinct right for the data subjects who should be able to ask for the restriction of processing in other cases than the two situations foreseen in paragraph 3 of Article 16, especially in cases where erasure will have been refused by the controller without restricting the processing.

If a request for erasure or rectification is refused, national legislation must require controllers to provide written information regarding the refusal as well as the reasons for the refusal. Article 16(4) provides the option for Member States to legislate to restrict, either fully or partially, the written information to be provided to the data subject concerning the refusal by the controller to rectify or erase the data or to restrict the processing and the reasons for this refusal.

Although the Directive only foresees the possibility to restrict the provision of this information to the data subject in case of refusal by the controller, the WP29 underlines that it should be clear that in cases where it is established that the data are inaccurate or incomplete, or that data are processed in violation with Articles 4, 8 or 10 LED, the controller shall not be able to refuse the rectification or erasure of the data. In addition, the WP29 recommends that Member States also provide for the categories of processing and situations where the controllers will never be allowed to, wholly or partly, refuse to rectify or erase the data or restrict the processing. Indeed, without such national measures, the controllers would be in a position to decide themselves, without further criteria, when to refuse to rectify or erase the data, or restrict the processing.

Member States should ensure that controllers always provide an answer to a right to erasure or rectification request and that if the right is being restricted or denied, the data subject is provided with the information regarding the right to lodge a complaint with a supervisory authority or the option to seeking a judicial remedy. As this information will lead to the only enforceable right in cases where the right to information that the rights to rectification or erasure have been restricted will have been itself restricted, the information provided to data subjects in this regards must be done so in a reasonable time frame and in a clear and intelligible manner.

The WP29 would like to remind again the national legislators that any exemptions from the fundamental rights and legitimate interests of the natural person should be applied as the exception rather than the rule and interpreted in a restrictive manner, as regularly recalled by the ECtHR including concerning the limitations of the rights of data subjects in the context of processing which would fall in the scope of the Directive[12].

Where a controller finds personal data to be inaccurate, that controller must ensure that the rectification of that data is communicated to the original controller who collected the personal data. In addition, the WP29 recommends that the controller also informs the data subject of the rectification, erasure or restriction of processing of his / her data, in line with what is foreseen in Article 12(3).

Where personal data has been rectified, erased or processing has been restricted, the controller must notify any recipients of that data. Those recipients must also similarly rectify, erase or restrict the processing of that personal data. As the Directive does not give any indication as to when this information should be sent, WP29 stresses that this information should be given as soon as possible in order to avoid any adverse effect for the data subject who exercised his or her rights.

6. Indirect access (Article 17)

In accordance with Article 17(1), national legislation have to foresee the possibility to exercise the rights to information, access, or information about refusal of rectification or erasure by the controller through the competent supervisory authority when these rights have been restricted by the controller on the basis of legislative measures allowing for restrictions, and not where these rights could be exercised directly with the controller.

In addition, the WP29 would like to recommend, accordingly to its recommendation to provide for categories of processing and situations where the right to rectification or erasure will have been wholly or partly restricted by the controller (see supra Article 16(4)) through national measures, although it is not expressly foreseen by the Directive, that in such cases national law should also provide that the competent supervisory authority shall also be able to exercise these additional rights for the data subjects.

This right to have their rights exercised through the competent authority has to be seen as an additional guarantee offered to the data subjects in the context of the Directive, where the GDPR does not foresee such possibility when rights will have been restricted. However, the WP29 underlines that this additional avenue to exercise their rights complements their right to lodge a complaint with a supervisory authority or to seek judicial review.

[12] See for instance S. and Marper against UK, ECHR, 2008, or M.K against France, ECHR, 2013

Controllers must inform data subjects of the possibility to exercise their rights through the supervisory authority (17(2)) and therefore in order to facilitate the exercise of this right this information should be clear, intelligible, given as soon as possible by the controller to the data subject, and include the contact details of the competent supervisory authority.

Furthermore, controllers should keep registers of requests. Such registers could be kept either by the DPO or by the DPA. In addition, DPAs should also document all requests on indirect access e.g. in a register to be able to keep track of them and in order to collect statistic data.

Under Article 17(3), competent supervisory authorities engaged in exercising these rights must at least inform the data subject that all necessary verifications or a review have taken place and that he or she has the right to seek a judicial remedy. The WP29 would recommend that in ordinary circumstances these pieces of information should be given jointly, including where possible the precise information as to which judicial authority is competent, either by providing its contact details and/or the reference of the relevant legal provision in order to facilitate the data subjects' enquiries.

In addition, the WP29 recalls that the possibility for data subjects to exercise their rights through the competent supervisory authority remains distinct from, and has to be provided for, in addition to the right to bring a complaint to the supervisory authority, which shall always be available to data subjects

Recommendations of the WP29

1. The Directive provides for a new architecture of the rights of data subjects, the principle being that they have a right to information, access, rectification, erasure or restriction of processing, unless these rights are restricted. Such restrictions shall only be possible where they constitute a necessary and proportionate measure and interpreted in a restrictive manner. Where these rights will have been restricted, Member States shall provide for the possibility for data subjects to exercise their rights through the competent supervisory authority which constitutes an additional safeguard for the data subjects.

2. The Directive states that Member States must provide for data subjects to have the right to obtain confirmation of processing and access to personal data being processed from the controller. The Directive does not allow for blanket restrictions to data subject rights.

3. National legislators and controllers should bear in mind the necessity to ensure as far as possible that accurate data is processed and that founded requests to rectify data are processed with necessary urgency.

4. In addition to the right to obtain the restriction of processing instead of erasure, Member States should also provide for an autonomous right to the restriction of processing for data subjects in their national legislation, especially in cases where erasure will have been refused by the controller.

5. Restrictions to the right to rectification, erasure or restriction of processing should be documented and in case of a restriction of processing data should also not be sent to other controllers until the restriction is lifted.

6. In cases where it is established that the data are inaccurate or incomplete, or that data are processed in violation with Articles 4, 8 or 10 of the Directive, the controller shall not be able to refuse the rectification or erasure of the data.

7. The Directive only expressly foresees the possibility for Member States to restrict the information to be provided by the controller in case of refusal to rectify or erase the data or restrict the processing. However, Member States should also provide for the categories of processing and situations where the controllers will never be allowed to, wholly or partly, refuse to rectify or erase the data or restrict the processing.

8. The possibility for data subjects to exercise their rights remains complementary to their right to lodge a complaint with a supervisory authority or to seek judicial review.

9. Controllers and data protection authorities should keep registers of requests.

10. Where competent supervisory authorities exercise their rights on behalf of data subjects, they must at least inform the data subject that all necessary verifications or a review have taken place and of their right to seek a judicial remedy. In ordinary circumstances these pieces of information should be given jointly.

Article 25
Logging

Key topics

1. Objective of logs
2. Content of logs and justification of access
3. Use of logs for criminal proceedings
4. Storage period for logs
5. Log archiving

1. Objective of logs

According to Article 25, national laws should envisage an obligation to keep logs for, as a minimum, processing operations as collection, alteration, consultation, disclosure including transfers, combination and erasure carried out in automated processing systems. Furthermore, in case of consultation and disclosure, the logs 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 implementation of logs is a crucial tool for data protection monitoring, hence for controlling all relevant data processing operations. In order to do so, it should be possible to trace the users' activity to spot abusive use. National laws shall then further develop on the requirements for logging: on content, on storage periods, on technical measures, on self-auditing and on internal policies to promote compliance.
Taking into account the objective of the logs, national laws should determine the adoption of technical measures to guarantee the integrity of the logs; otherwise they would become useless.

Logging has a two-fold goal once it can be used as a deterrent action of non-authorised use, which can only be effectively if a log analysis rule is implemented, and a punitive action when a breach is discovered. Therefore an additional aspect to be considered is the enhancement of the controllers self-auditing activity through periodical reports of log analysis, which could be done in an automated manner and tailor made for specific areas of law enforcement work.

2. Content of the logs and justification of access

The necessary contents of the logs on access i.e. consultation and disclosure should make it possible to establish not only date and time of such operations, but also the justification and the identification of the person who consulted or disclosed the data and the identity of the recipient in case of disclosure.

In the view of the WP29, the identification of the individual user should not be limited to the operations of consultation and disclosure, but foreseen for all processing operations and include every person involved, for example the activities of an outside organisation which is involved in troubleshooting or forensic activity.

Regarding the obligation to make it possible to establish the justification of access i.e. consultation and disclosure, to a certain extent the content of the logs will depend on the system or application generating them. As this will be subject to different national configurations, the Directive does not give any more specifics. But in the end, there has to be something in the logs explaining the reason why an individual accessed that log or

record. In the view of the WP29, this obligation can best be fulfilled by ensuring that any automated processing systems and their respective logging elements are developed in accordance with the "data protection by design" requirements specified in Article 20 of the Directive. The logging requirements of Article 25 should therefore be taken into account when designing the access regime to the respective database, system or application. The person who consults specific data could be obliged to give an explanation before getting access, so that the content of this explanation can be transferred into the logs as justification. In any case, this obligation is technically challenging and needs some preparation. This is why the legislator granted a longer implementation period to comply with Article 25 (2).

3. Use of logs for criminal proceedings

Article 25 (2) lays down the sole purposes for which logs can be used. Besides the verification of lawfulness of processing, self-monitoring and ensuring the integrity and security of the personal data, logs can also be used for criminal proceedings.

Considering the very limited and precise use of logs and, consequently, a very restricted regime of access to logs, WP29 interprets the disposition providing for the use of logs in criminal proceedings whenever those proceedings are related to the purposes of the logs as described above. This would be a logical assumption as any illicit practices in data processing that are exposed through the analysis of logs are likely to be subject to criminal proceeding.

Therefore, without prejudice to the powers of judicial authorities when acting in their judicial capacities, we should consider adequate to use logs in criminal proceedings when the lawfulness of a data processing operation - for instance, data consultation or disclosure - is being challenged, when there is a security breach in dispute or if data integrity is at stake.

In conclusion, Article 25 (2) should be read narrowly as to the use of logs, having in mind the actual objectives of logs and the potential need to investigate and prosecute a criminal data breach.

4. Storage period for logs

The Directive does not set any requirement on the storage period for logs. Therefore, in the view of the WP29, national legislators should provide for adequate storage periods by giving clear criteria or setting fixed periods.

An adequate storage period for logs has to be derived from the purposes of logging as laid down in Article 25 (2) and should ensure that it is possible to achieve those purposes. This goes especially for the verification of the lawfulness of the processing,

which lies within the tasks of the DPAs. Therefore, the storage period for logs should give DPAs enough time to retrace and review the data processing.

In the view of the WP29, the monitoring of access to data i.e. consultation and disclosure should be done on a regular basis and within a shorter period of time. In general, it is not necessary to keep the logs on access as long as the underlying data are stored.

As for the logs on the history of data i.e. collection, alteration, combination and deletion, a different approach may be adequate depending on the database in question.[13]

Deciding on appropriate storage periods, it should be taken into account that on the one hand, a long storage period for logs will help to keep trace of the history of the processing (with a benefit for the data subject, the quality of data and the security measures). In criminal procedures or for preventive purposes the underlying data are usually stored over a long period and often the data subject only gains knowledge of the processing at a later stage. At this point it should be possible to retrace the data processing by means of the logs. On the other hand, keeping the logs after deletion of the underlying data implies that part of the information is also retained for longer than the storage period foreseen. This would call for a shorter storage period of logs. In conclusion, the right balance should be found on a case-by-case basis.

5. Log archiving

Furthermore, it is possible that the adequate storage period for logs could be different to that which the original source of the logs could support. In such cases the use of log archiving should be considered, and - depending on the context - may even be required (e.g. for compliance with other requirements of the Directive). For example, there may be a finite period that logs from a particular system or application could be stored until they are overwritten, either due to time or storage space, so archiving what is necessary for the purposes of the Directive may be one way of ensuring that controllers retain the required information for however long is required.

Recommendations of the WP29

1. National laws shall further develop on the requirements for logging: on content, on storage periods, on technical measures, on self-auditing and on internal policies to promote compliance.

[13] For example, in the SIS II framework, there is a different regime of storage periods for logs concerning alerts and logs concerning access made by persons. The logs concerning access made by persons are to be deleted at the earliest one year after their creation, and at the latest after three years. In contrast, the logs on the history of alerts are to be erased one to three years after deletion of the respective alert. Another approach is chosen in the framework of the Europol Convention, which foresees deletion of all logs after three years regardless of the underlying processing operation.

2. In the view of the WP29, the identification of the acting person should not be limited to operations of consultation and disclosure, but foreseen for all processing operations. The logging requirement concerning justification of consultation and disclosure should be implemented in the technical design of the source system and its access regime (data protection by design).

3. Without prejudice to the powers of judicial authorities when acting in their judicial capacities, the use of logs in criminal proceedings can only be considered adequate when the lawfulness of a data processing operation - for instance, data consultation or disclosure - is being challenged, when there is a security breach in dispute or if data integrity is at stake. The use of logs for any other kind of criminal proceedings would be excessive and could undermine the real goals of the logging activity.

4. When deciding on appropriate storage periods, the right balance should be found on a case-by-case basis depending on the data base in question, taking into account on the one hand, that a long storage period for logs will help to keep trace of the history of the processing and on the other hand, that when keeping logs for longer than the underlying data, part of the information is kept even longer.

5. The use of log archiving should be foreseen where the original source of the logs is not capable of supporting the adequate storage period for logs.

Article 47
Powers of data protection authorities

Key topics
1. Effective powers
2. Common supervision over the Directive and the GDPR

1. Effective powers

According to Article 47 Member States have to provide by law for DPAs to have effective powers for investigations (Article 47(1)), effective corrective powers (Article 47 (2)) and effective advisory powers (Article47(3)) as well as the power to bring infringements of provisions adopted pursuant to the Directive to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings, in order to enforce the provisions adopted pursuant to the Directive.

Unlike the GDPR, the Directive does not enumerate and define the investigative, corrective and advisory powers in detail. In the view of the WP29, the GDPR and the

Directive should nevertheless provide a similar level of protection and thus equivalent rules on key issues. Therefore the WP29 recommends that national laws transposing the Directive regulate these powers in a similar way to the GDPR, as far as possible.

With regard to corrective powers, Article 47(2) only gives examples of what these powers could be, like the power to order the erasure or rectification of data or to impose limitations or bans on processing, and the crucial attribute of being "effective". In the view of the WP29, this attribute calls for binding powers of DPAs to warn, impose or order certain corrective actions and issue binding decisions against controllers. DPAs may not in general be limited to non-binding and non-enforceable acts like pure complaints or objections. In such cases the national implementation of the Directive must be considered as insufficient.

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 Article 47(5). Such legal proceedings are supposed to be additional instruments and not alternative instruments to effective corrective powers.

Furthermore the WP29 wishes to recall the CJEU *Schrems*-judgement of 6th October 2015, C-362/14. According to paragraph 65 of the judgement, when examining a claim against data transmissions based on an adequacy decision and finding the objections well-founded, the competent national supervisory authority must have the power to put forward those objections before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity. In the light of this ruling, when claims concern the validity of adequacy decisions, the national legislator has to foresee that supervisory authorities have the power to bring the matter to court. This must apply to adequacy decisions based on Article 36 LED as well.

2. Common supervision over LED and GDPR

Another aspect that could substantially affect the efficiency of the supervision is the national decision of each member state whether to establish a separate data protection authority for the Directive. Pursuant to Article 41(3), the Member States may provide for the supervisory authority established under the GDPR to be also the supervisory authority referred to in the Directive. In the view of the WP29, such an approach should be strongly encouraged.

Entrusting a single data protection authority with the supervision of both the GDPR and the Directive will guarantee that the common principles and concepts in the two legal acts are interpreted homogeneously and will ensure consistency of the data protection policy and practice. Furthermore, the choice of one supervisory authority will smooth

the functioning of the European Data Protection Board and will avoid the risk of further stretching limited human and financial resources of the data protection authorities.

This is without prejudice to the possibility for some Member States to establish more than one supervisory authority, to reflect their constitutional structure, namely the federal states.

Recommendations of the WP29

1. National laws have to foresee effective investigative, corrective and advisory powers and in addition the power to bring infringements to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings. The WP29 recommends that national laws detail the powers of DPAs in line with the powers foreseen in the GDPR.. When claims concern the validity of adequacy decisions based on Art. 36 of the Directive, the national legislator has to provide a direct way to court.

2. Member States should entrust a single data protection authority with the supervision of both the GDPR and the Directive. This is without prejudice to the possibility to reflect their constitutional structure, namely the federal states.