ARTICLE 29 DATA PROTECTION WORKING PARTY

3211/15/EN
WP 233

Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

Adopted on 01 December 2015

General remarks

Applicability of the Charter of Fundamental Rights of the European Union to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties

Article 8 of the Charter of Fundamental Rights of the European Union (hereafter "The Charter"), states that personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". Article 8(3) of the Charter states that compliance with these rules shall be subject to control by an independent authority.

According to Article 52(1) of the Charter, "Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. As the Court of Justice of the European Union (hereafter 'CJEU') has recently reiterated in its Schrems judgment and in Digital Rights Ireland and Others judgment[1], interferences in the private life of individuals and in the right to protection of personal data shall be limited to what is strictly necessary and proportionate to the objectives of general interest foreseen, i.e. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[2].

The Article 29 Working Party (hereafter: WP29) recalls that these rights and CJEU's corresponding case law apply to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and insists that it is duly transposed into the principles set out in the Directive.

In this regard, the current Council text of the draft directive raises concerns in that it does not ensure that interferences in the private life of individuals and in the right to protection of personal data are limited to what is strictly necessary.
More specifically, as will be laid out in further detail below, the WP29 notes that personal data processed in a law enforcement context could be further processed for incompatible purposes.

Moreover, the data controller is not required to distinguish between different categories of data subjects, and that personal data of children are not subject to specific safeguards. There is no obligation to carry out a data protection impact assessment in advance of setting up new data processing, the rules for the transmission and use of the data to private parties and third countries are not properly defined and data could be used to create profiles or single out a person or a category of persons on the sole basis of sensitive data. Additionally, with regard to the security of the data processing, risks posed by data breaches are left to the assessment of data controllers and logging is subject to exceptions. Finally, the powers of competent supervisory authorities are insufficiently detailed.

[1] Judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, paragraph 52
[2] C-362/14 – 6 October 2015, consideration 92

Should these shortcomings remain in the final text of the directive, it could have highly detrimental consequences for individuals and risks that the text is contrary to both Article 8 of the European Convention of Human Rights[3], Articles 7 and 8 of the Charter, the European Convention for the protection of individuals with regard to automatic processing of personal data.

The WP29 insists that setting out rules which respect the principles as established in the Charter and, more generally, in the applicable data protection framework will not only benefit data subjects but also data controllers in their daily work.

Recommendation No. R(87)15 principles as a minimum required when setting out an equivalent legal framework at EU level.

At the European level, the protection of individuals with regard to the processing of personal data by competent authorities for purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties is already dealt with in specific texts: Council Framework Decision 2008/977/JHA of 27 November 2008 (hereafter "Framework Decision 2008/977/JHA") at EU level and Recommendation No. R(87)15 of the Committee of ministers to Member States regulating the use of personal data in the police sector[4] at Council of Europe level (hereafter "Recommendation No. R(87)15")[5].
The principles of data protection laid down by the Framework Decision 2008/977/JHA are limited to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, whereas Recommendation No. R(87)15 provides a specific and more complete set of rules.

The WP29 therefore advises that Recommendation No. R(87)15 be considered as the minimum required when setting out an equivalent legal framework at EU level.

Risks inherent to law enforcement activities and resulting necessary safeguards

WP29 has used its experience and relevant CJEU and ECHR case law[6] to develop its view that personal data processing which, in the general/common context, might not be perceived

[3] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950
[4] Recommendation No.R(87)15 regulating the use of personal data in the police sector adopted by the Committee of Ministers of the Council of Europe on 17 September 1987 at the 410th meeting of the Ministers' Deputies.
[5] Recommendation No.R(87)15 has been used as a benchmark for setting the level of data protection in texts regulating the Schengen Information System and EUROPOL.
[6] See in particular CJEU judgment on the data retention directive in Joined Cases C-293/12 and C-594/12Digital Rights Ireland and Seitlinger and Others.
See also ECHR: "The compiling, storing, using and disclosing of personal information by the State, for example in respect of a police register, amounts to an interference with one's right to respect for private life as guaranteed by Article 8 §1 of the Convention (Leander v.Sweden, 26 March 1987, §48, Series A no. 116). The subsequent use of the stored information has no bearing on that finding (Amann v. Switzerland [GC], no. 27798/95, §69, ECHR 2000-II). Such interference breaches Article 8 unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 of Article 8 and, in addition, is " necessary in a democratic society" to achieve those aims.
In the case of **M.K. v. France** (application no. 19522/09) of 18 April 2013, the European Court of Human Rights held, unanimously, that the retention of the fingerprints of a French national who had been the subject of two investigations concerning book theft, which ended in one case with his acquittal and in the other with a decision not to prosecute, **violates Article 8** (right to respect for private and family life) of the European Convention on Human Rights The Court considered, in view of the circumstances of the case, that the data in question amounted to disproportionate interference with the applicant's right to respect for his private life.
In the case of **S. and Marper v. the United Kingdom** (application nos. 30562/04 and 30566/04) of 4.12.2008, the Court found that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular

as a threat to fundamental rights may require particular attention when carried out in a law enforcement/judicial context, as the risks to fundamental rights become greater. Far from justifying less stringent requirements, or derogating from the common duty, such processing which entail a limitation on the fundamental rights of the individuals concerned as laid down in Article 52 (1)[7] of the Charter and, as a result, must be carried out in full compliance with the core principles of data protection. The use of exemptions or restrictions should be exceptional and interpreted narrowly, particularly as it concerns the full exercise of the rights of individuals. Personal data shall be processed with sufficient guarantees and safeguards providing full accountability and transparency towards individuals[8].

Consistency between both texts

The WP29 insists on the importance of considering both the draft regulation and the draft directive as part of a package to ensure the necessary consistency between both texts.

As an illustration, a lower degree of obligations laid down on the controller with regard to DPIAs, data breaches and data subject's rights in the draft directive could result in difficulties for data controllers who process data under the scope of both the regulation and the directive.[9]

The WP29 therefore recalls its recommendation to ensure "that the 'core' aspects of both texts are consistent and uniformly understood, irrespective of the legal instrument chosen in order to avoid confusion and overlap impacting the level of protection guaranteed to individuals". [10] In particular, the definitions, principles, obligations, individual's rights and powers of

samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, failed to strike a fair balance between the competing public and private interests, and that the respondent State had overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention in question constituted a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society. The Court concluded unanimously that there had been a violation of Article 8 in this case.
More recently, in the case of **M.M. v. the United Kingdom** - 24029/07 of 13.11.2012, the Court was not satisfied that there were sufficient safeguards in the system for retention and disclosure of criminal record data to ensure that data relating to the applicant's private life would not be disclosed in violation of her right to respect for her private life. The retention and disclosure of the applicant's caution data accordingly could not be regarded as having been in accordance with the law.
See also B.B. v. France (application no 5335/06), Gardel v. France (no 16428/05), M.B. v. France (no 22115/06), where the ECHR found that the inclusion in national sex offender database did not infringe the right to respect for private life and there was no violation of article 8 (right to respect for private and family life)of the European Convention on Human Rights.

[7] Article 52(1) of the Charter states that :"Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. See above development on the Charter

[8] See CJEU judgment on the data retention directive: "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"

[9] Examples of these situations are the transfer of PNR data and data on financial transfers to law enforcement authorities. In Annex III of the Impact Assessment of both proposed instruments, Framework Decision 2008/977/JHA is strongly criticised for failing to address the legal uncertainty for situations in which data collected for commercial purposes are used for law enforcement purposes.
This also applies to other situations, for instance when information is transferred between a law enforcement authority and a private entity or when a law enforcement authority would transfer data to another public authority not responsible for law enforcement.

[10] WP29 opinion relating to the core topics in the view of trilogue, 17 June 2015, see in particular top of page 3 (available following this link: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf)

supervisory authority shall be consistent and exceptions foreseen in the draft directive limited to what is strictly necessary.
This consistency is even more important considering the growing number of situations in which activities of the private sector and of the law enforcement sector interact with each other[11].

Specific comments

1/ Subject matter and objectives

As observed already in its opinion[12] on the core issues of the Regulation, in order to ensure a consistent and high level of protection, the WP29 considers that the processing activities performed by the competent authorities for purposes not linked to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be clearly maintained under the scope of the Regulation.

In this regard, the WP29 recalls that an extension of the scope of the Directive, as proposed by the Council of the EU, to all processing activities for the "safeguarding against and the prevention of threats to public security" - in addition to processing activities carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties- would result in a different level of protection depending on its implementation by Member States[13].

Moreover, the notion of "the prevention of threats to public security*"* not linked to the concept of criminal offences is quite vague and may include types of processing operations just because they are carried out by controllers that operate in the widest context of law enforcement and even public security. For example, the WP29 recalls that, in some Member States, public health is included in public security in its administrative meaning.

Additionally, such extension would include an indefinite number of authorities whose tasks may be only occasionally linked to that purpose into the scope of the directive which would result in a lower level of data protection in the public sector from the one proposed by the Regulation. There is no compelling reason to create such flexibility and to exclude the activity of public security from the Regulation.

The WP29 therefore supports Commission and European Parliament versions of Article 1 limiting the subject matter and objectives to the processing of personal data by competent

[11] Examples of these situations are the transfer of PNR data and data on financial transfers to law enforcement authorities. In Annex III of the Impact Assessment of both proposed instruments, Framework Decision 2008/977/JHA is strongly criticised for failing to address the legal uncertainty for situations in which data collected for commercial purposes are used for law enforcement purposes.
This also applies to other situations, for instance when information is transferred between a law enforcement authority and a private entity or when a law enforcement authority would transfer data to another public authority not responsible for law enforcement.[12] WP29 opinion relating to the core topics in the view of trilogue, 17 June 2015 (available following this link: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf)
[12] WP29 opinion relating to the core topics in the view of trilogue, 17 June 2015 (available following this link: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf)
[13] The WP29 already expressed this position in its letter relating to the core topics in the view of trilogue published on 17 June 2015 (see http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf)

authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties

2/ Fairness of the processing

Fairness of the processing is a standard principle guaranteed in the majority of the texts dealing with data protection. In this particular and very sensitive context where Member States apply their coercive powers, it is even more important that no doubts exist as to the fairness of the processing.

The WP29 therefore welcomes and supports that the text of the draft directive establishes the fairness of the processing as a prior and key principle.

As part of this fairness requirement and to comply with principle 2.3[14] of Recommendation No.R(87)15 of the Council of Europe, the WP29 recommends that specific legal provisions lay down powers to collect data by technical surveillance or other automated means to ensure fairness of data processing carried out in such context.

3/ Purpose limitation

WP29 notes that purpose limitation is a key data protection principle designed to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further, different use. The controller must only collect data for specified, explicit and legitimate purposes, and once data are collected, they must not be further processed in a way incompatible with those purposes. Principle 4 of aforementioned Recommendation No.(87)15 formulated this as follows: "[...] personal data collected and stored by the police for police purposes should be used exclusively for those purposes".

As a result, data collected for a specific crime may also be used by competent authorities for solving another crime provided that compatibility is assessed on a case by case basis and subject to a legal basis including clear and explicit safeguards.

However, the WP29 insists that law enforcement, *per se*, shall not be considered as one specified, explicit and legitimate purpose.

Furthermore, purpose limitation and distinguishing between different categories of personal data[15] are intrinsically interlinked. Specific data or data on specific categories of data subjects might be necessary in certain criminal investigations. However their further use should be limited and strictly conditioned, in particular where the relation between a person and a crime is not established (the collection of data on this person is related to a crime but they are not classified as suspects, victims and witnesses). More specifically, contrary to data relating to suspects or convicted persons, the further use of data relating to "non suspects" should be prohibited.

Such a restriction should also apply to the processing of sensitive data. Although they proved necessary for the crime for which they were collected, their necessity to the further use of the data should be demonstrated.

[14] Recommendation No.R(87)15 regulating the use of personal data in the police sector, Principle 2 "Collection of data": The collection of data by technical surveillance or other automated means should be provided for in specific provisions

[15] See development on ddistinction between the different categories of data subjects

The Working Party insists that any processing for a purpose different than the specific one for which the data was originally processed should always have its own legal basis including clear and specific safeguards.

4/ Data minimization

WP29 recalls that only the minimum amount of personal data should be processed to achieve the purpose set out; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not constitute personal data. WP29 refers to recommendation No R(87)15 which states in principle 2.1 that the collection of personal data for police purposes should be limited to that which is necessary for the prevention of a real danger or the prevention of a specific criminal offence. The WP29 insists that the principles of necessity and proportionality be considered when processing personal data in a law enforcement context and that such processing must not result in the massive and indiscriminate collection and further processing of personal data even where made possible by new technologies.

In this regard, the WP29 supports Article 4(c) in the version of the European Parliament specifying, amongst the principles relating to personal data processing, that the data processed should be adequate, relevant and "limited to the minimum necessary for which they are processed" and that "they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data".

5/ Distinction between the different categories of data subjects

WP29 supports a substantial provision of the directive distinguishing between different categories of data subjects (suspect, perpetrator, victims, witnesses, informants, contacts and accomplice). As already highlighted in its opinion 01/2013 providing further input into the discussions on the draft directive[16], such a distinction is also necessary to ensure proper implementation of the principles relating to data processing. It also insists on the crucial importance of updating those data at the end of the investigation/judicial proceeding. EU policies and legislation which focus on fighting trafficking in human beings and have a victim-centered approach oblige data controllers to make proper distinctions. Without an obligation to introduce such distinctions, such policies will be less or not effective.

In its aforementioned opinion 01/2013[17], WP29 insisted, in particular, on the category of persons which have no known relation to a crime, the so-called "non suspects". Processing of data of persons who are not suspected of having committed any crime (other than victims, witnesses, informants, contacts and associates) shall be strictly distinguished from data of persons related to a specific crime and "should only be allowed under certain specific conditions and when absolutely necessary for a legitimate, well-defined and specific purpose." Furthermore, such processing should (in the view of the data protection authorities) "be restricted to a limited period and the further use of these data for other purposes should be prohibited." A specific protection of "non-suspects" is particularly required when the processing is not done in a specific criminal investigation or prosecution.

[16] Opinion 01/2013, 00379/13/EN WP201 of February 2013, providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_en.pdf

[17] Opinion 01/2013, 00379/13/EN WP201 of February 2013, providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_en.pdf

The Working Party already suggested introducing an article in this regard[18] and therefore supports Article 5 as laid down in the version of the European Parliament obliging the controllers to clearly distinguish between personal data of different categories of data subjects (suspect, perpetrator, victims, witnesses, informants, contacts and accomplice). This would ensure that data inserted in police databases is accurate and regularly updated with regard to the categorization, and to make the processing of data of these different categories subject to specific conditions. .

6/ Special categories of data

The Working Party considers that the processing of sensitive data should be prohibited as a principle and exceptions granted subject to strict conditions. In this regard, the Working Party recalls Principle 2 of Recommendation 87/15 following which "the collection of data on individuals solely on the basis particular racial origin, particular religious convictions, sexual behavior or political opinions or belong to particular movements or organizations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry."
The processing of special of categories of data could therefore be authorized when:

- (a) the processing is authorised by a law providing appropriate safeguards ***strictly necessary and proportionate for the performance of a task carried out by the competent authorities for the purposes set out in Article 1(1), on the basis of Union or Member State law which shall provide for specific and suitable measures to safeguard the data subject's legitimate interests, including specific authorisation from a judicial authority, if required by national law***; or

- (b) the processing is necessary to protect the vital interests of the data subject or of another person; or

- (c) the processing relates to data which are manifestly made public by the data subject**,** ***provided that they are relevant and strictly necessary for the purpose pursued in a specific case***.

The Working Party considers that the processing of sensitive data should be prohibited as a principle and exceptions granted subject to strict conditions. Therefore, the WP29 supports Article 8 in the version of the European Parliament.

Genetic and Biometric data

The WP29 welcomes that genetic data are defined in Article 3 and considered as a special category of data. It insists that creating general genetic profiles outside of any specific investigation should be strictly prohibited.
As biometric data can identify a person automatically and uniquely by using one or more of his physical, physiological or behavioral characteristics, they are not like any other personal data and should be afforded greater caution[19], as they enable identification on the basis of a

[18] See aforementioned Opinion 01/2013, 00379/13/EN WP201 of February 2013 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_en.pdf

[19] In the case of S. and Marper v. the United Kingdom (application nos. 30562/04 and 30566/04), the Court gave its views on the processing of genetic and biometric data. It first noted that, given the nature and the amount of personal information contained in cellular samples, their retention per se had to be regarded as interfering with the right to respect for the private lives of the individuals concerned. In the Court's view, the capacity of DNA profiles to provide a means of identifying genetic relationships between individuals was in itself sufficient to

biological reality which cannot be changed, revoked or cancelled. Besides, biometric data processing often includes collection (cf. cases where fingerprints are not readable) and quality issues leading to false positives (cf. automated border control).

The processing of biometric data therefore requires stricter data protection requirements in particular regarding data quality, accuracy and security.

The Working Party stresses that, similarly to other « sensitive » data (e.g. genetic data), biometric data should be defined in Article 3 and covered by Article 8.

7/ Processing of data relating to children

Processing personal data for law enforcement purposes might pose additional risks for children, a particularly vulnerable collective. Their best interest should be a primary consideration for Member States when applying this Directive, in accordance with Article 24(2) of the Charter of Fundamental Rights of the European Union[20]. The WP29 considers that the processing of data relating to children requires the adoption of strengthened safeguards, including stricter storage periods and regular assessments of the effectiveness of such a processing. The possibility to secure the educational and moral recovery of juvenile offenders by allowing, in certain cases, the possibility to ask the erasure or to block the use of those data should also be given. Member States should be allowed the flexibility for these safeguards to be set out in line with domestic legislation while assuring the highest degree of protection. The WP29 therefore recommends introducing specific provisions in this regard.

The WP29 supports a text introducing additional safeguards when processing personal data relating to children such as, for example: "The measures taken by the data controller shall in particular include drawing up and implementing specific safeguards in respect of the treatment of personal data relating to children, where appropriate." [21] This particular attention given to children's personal data shall also be a primary concern when carrying out a data protection impact assessment.

8/ Profiling

As a minimum, no profiling or automated decisions shall be made on the sole basis of sensitive data. In that sense, the WP29 regrets that this safeguard has been omitted in the text approved by the Council.

The data subject should always have the right to contest any decision taken by automated means and express their views.

The WP29 supports Article 9(2) in the versions of the Commission and European Parliament prohibiting the profiling done on the sole basis of sensitive data.

---

conclude that their retention interfered with the right to the private life of those individuals. The possibility created by DNA profiles for drawing inferences about ethnic origin made their retention all the more sensitive and susceptible of affecting the right to private life. The Court also considered that fingerprints contain unique information about the individual concerned and their retention without his or her consent cannot be regarded as neutral or insignificant. The retention of fingerprints may thus in itself give rise to important private-life concerns and accordingly constituted an interference with the right to respect for private life.

[20] Article 24(2) of the Charter of Fundamental Rights of the European Union, the Rights of the child: "In all actions relating to children, whether taken by public authorities or private institutions, the child's best interest must be a primary consideration". [21] See Article 18(da) of EP's version of the text.

[21] See Article 18(da) of EP's version of the text.

9/ Data subjects rights

The WP29 recommends that individual's rights be clearly defined and established in substantive articles as a principle and that limitations to these rights should be justified on a case by case basis, according to the sensitivity of the data processed or the potential consequences of the exercise of those rights on an ongoing investigation or procedure. The legislator and/or the supervisory authority, where it is entrusted with prior notification competences, should have the opportunity to assess whether this limitation is justified and where setting out an indirect access right would be relevant. In any case, the supervisory authority should have the opportunity to supervise a posteriori the modalities of exercise of these rights, whether direct or indirect.

Information to the data subject

In order to enable the data subject to challenge the legality of the processing of personal data concerning her or him, and without prejudice to legitimate exceptions, the WP29 strongly supports the right of the data subject to be informed as a principle, particularly where the data are collected without her or his knowledge. This principle should only be exempted when such information would jeopardize ongoing investigations, expose a person to a danger or harm the rights and freedoms of others. This right is particularly important for witnesses and non-suspects.

In these cases, the information should be provided to the data subject as a harmonized standard and should comprise at least the items covered by the Commission proposal[22].

Right of access for the data subject and limitations to the right of access: the establishment of a right to indirect access

Where a direct access would jeopardize ongoing investigations, expose a person to a danger or harm the rights and freedoms of others, the possibility should be left to Member States to provide for indirect access.

The right of access should include, as an integral part of the minimum set of information to be provided, subject to duly justified exceptions, the right of the data subject to obtain from the controller a copy of the personal data undergoing processing as well as intelligible information about the logic involved in the automated processing, at least in the case of the measures related to Article 9 on automated individual decision making.

The WP29 supports Article 12 in the version of the European Parliament detailing the information to be provided upon access request and Article 13 in the same version in so far as it ensures that limitations to the right of access may be made use of only after assessing the specific case.

Right to object

WP29 understands that for most processing carried out by police or judicial authorities, the right to object to the processing should not be allowed, in order for the public function to proceed. However, situations can arise where some individuals (e.g. victims or witnesses)

[22] the identity and the contact details of the controller and of the data protection officer if any; the purposes of the processing for which the personal data are intended; the data retention period; the existence of the right to request from the controller access to and rectification, erasure or restriction of processing; the right to lodge a complaint with a supervisory authority and the recipients or categories of recipients of the personal data

should be allowed to object to the processing of their personal data (e.g. after the completion of the justice process). Such possibility exists in Europe and, as such, the WP29 calls for the text of the Directive to acknowledge this important individual right.

The WP29 therefore supports a text allowing for such right to be set out for categories of data subjects such as victims and witnesses.

10/ Data controllers and processors' obligations

Data Protection Impact Assessment (DPIA)

The WP29 expresses its strong support for setting out a systematic DPIA approach in the field of law enforcement processing of personal data[23]. This obligation is even more relevant because the data controller is, according to the current text, supposed to assess himself, possibly with the help of the DPO, the risk posed by the processing to determine whether or not it will consult the supervisory authority.

This DPIA should be part of the impact assessment carried out prior to setting up a data processing which should not only involve data protection but also considerations on the wider impact of the data processing envisaged on the rights and freedoms of the data subjects.

The WP29 welcomes the amendment of the European Parliament in Article 25a setting out a framework to require data controllers to carry out a DPIA[24].

Logging

The WP 29 reminds that the keeping of logs is an essential element of accountability and transparency, linked to internal control and audit as well as to the monitoring of the lawfulness of the processing by supervisory authorities. It also enables the effective exercise of rights by data subjects. In that sense, in absence of detailed and understandable logs also safeguarded by measures aiming to maintain their integrity, the effectiveness of any kind of control would be seriously diminished.

The WP29 recalls the need to keep logs of processing operations in automated and non automated processing to ensure the traceabililty of the data processing and, in this regard, supports European Parliament's version of Article 24.

Prior consultation of the supervisory authority

As already stated in its opinion on the draft Regulation, the WP29 notes that the duty to carry out prior consultation with the supervisory authority is a power limited to some specified member states.

In view of the particular sensitivity of police and justice files, prior consultation of the supervisory authority is particularly necessary to safeguard the rights and freedoms of data subjects in many cases. Therefore, the WP29 is of the opinion that where supervisory authorities retain the potential to insist on prior consultation as a general principle, the absence of notification is the exception. For supervisory authorities who have been or are enabled to exercise a full prior check of the processing envisaged, this power should be maintained.

[23] In this regard, see WP29's detailed reasoning in aforementioned Opinion 01/2013.
[24] See Article 25(a) of the EP version of the draft directive

Having the option to carry out prior authorization, where it exists, should not detract from the requirement of supervisory authorities to provide advice to ensure respect for the fundamental rights to the protection of the individual's private life and their personal data. It should also not remove the power of supervisory authorities to inspect the data processing being conducted to ascertain compliance with data protection legislation.

The WP29 therefore advises maintaining a full prior check power for those supervisory authorities which have been or are enabled to exercise it under the current applicable legislation.

Security of the data processing

WP29 favors strict obligations concerning the security of personal data being processed. In this regard, it welcomes the obligations of the data controller regarding the keeping of documentation as well as the implementation of specific measures. However, the WP29 insists on the need for a provision allowing the adoption of minimum standards for the implementation of those security measures, notably encryption standards.

The WP29 therefore favors a text referring to the Commission setting out in implementing acts minimum standards for the implementation of security measures, notably encryption standards as set out in Article 27(3) of the Commission and European Parliament versions.

Data breach notifications

To the data subject

The WP29 supports different risk based thresholds for notification of personal data breaches to the individuals and would like to see an alignment with the wording of the ePrivacy Directive i.e. notification to the data subjects when the "personal data breach is likely to adversely affect the personal data or privacy of a data subject…" In this regard, the WP29 insists that exemptions to notification obligations to data subjects take account of the different categories of persons concerned by the processing. In particular, non suspects should be informed when the data breach puts them at risk.

To the supervisory authority

The risks inherent to data processing carried out by competent authorities for the prevention, detection or prosecution of criminal offences or the execution of criminal penalties are generally high. A data breach affecting such data is, therefore, likely to be highly detrimental to the individuals concerned. Such breaches may also be detrimental to Member States security as recent cases have shown.

For these reasons, the WP29 considers that, contrary to current Article 28(1) and 28(1)(a) of the Council version of the draft[25] directive, data breaches should be notified to the supervisory authority. Such notification shall be independent of the notification to the data subject.

[25] *Article 28 Notification of a personal data breach to the supervisory authority*
1. Member States shall provide that in the case of a personal data breach which is likely to result in a high risk for the rights and freedoms of data subjects**,** (...) the controller notifies, without undue delay (…) and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority (…). The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.

As a result, it favors a text which sets out a general obligation of notification to the supervisory authority. Being aware of the risks linked to divulging the existence of a data breach, the WP29 insists that supervisory authorities are subject to an obligation of confidentiality which will naturally apply in these cases.

The WP29 therefore favors the Commission and the European Parliament's versions of Article 28 setting out a general obligation of notification to the supervisory authority and distinguishing between categories of persons concerned as far as notification to the data subject is concerned and consequently.

11/ Transfers of personal data to third countries or international organizations

Transfers to third countries may take place only if the transfer is necessary for the prevention, investigation, detection or prosecution of specific criminal offences or the execution of criminal penalties in the framework of a specific investigation/procedure.

A strict prohibition of massive, repeated and structured transfers of personal data to third countries, a restrictive interpretation of exceptions and the systematic documentation of transfers.

In this regard, the WP29 favors the introduction of a strict prohibition on the massive, repeated and structured transfers of personal data to third countries authorities and reiterates that exceptions to the prohibition of transfers to inadequate countries should be interpreted restrictively. It supports article 36(2)(b) as introduced by the European Parliament, which states that: "*All transfers of personal data decided on the basis of derogations shall be duly justified and shall be limited to what is strictly necessary, and frequent massive transfers of data shall not be allowed".*

Documentation of transfers

In order to ensure that DPAs can properly check whether transfers are compliant with the requirements of the Directive and of national law, the Directive should also expressly foresee that the transfers are documented appropriately.

The WP29 therefore supports Article 23 stating that each controller shall maintain a record of the transfers of data to a third country or an international organisation, including the identification of that third country or international organisation. In this regard, the version of the European Commission and of the European Parliament referring to international transfers and not only categories of international transfers should prevail.

Consequences of the recent Schrems v. Data Protection Commissioner judgment

The WP29 insists that the CJEU's recent judgment in the Schrems v Data Protection Commissioner case[26] specifying the requirements of an adequate level of protection when personal data is transferred to third countries be taken into account when dealing with transfers of personal data to third countries under the directive regime. In line with the requirements set out by the judge, exceptions to the adequacy principle should be interpreted narrowly. According to the Court, Article 26(6) of Directive 95/46EC requiring such adequate

1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 29(3)(a) and (b). (…)

[26] C-362/14 – 6 October 2015

level of protection implements the express obligation laid down in Article 8(1)[27] of the Charter.

Considering the latter is applicable in a law enforcement context[28], the requirement for an equivalent protection of personal data presumably applies to transfers of personal data performed in such context as well.

In any case, the adequacy decision made by the Commission or a Member State shall be complemented by a full assessment of the police and justice sector and could be further assessed by the national independent supervisory authority when investigating a complaint.

The WP29 therefore advises the institutions to amend the relevant provisions accordingly.

In particular, it recommends maintaining in article 41(2)(a) of the proposed Regulation a specific reference to public security and criminal law as elements that should be taken into account by the Commission when assessing the adequacy of the level of protection[29]. The WP29 also suggests adding the following sentence in the head of Article 34(2): "… or the decision has not taken into account the data protection legislation applicable to the third country authorities competent for the purposes set out in Article 1(1), …"

It also suggests that the wording of Article 59 takes account of recent rulings of the Court of Justice of the European Union.

Transfers to public/private parties in a third country

The transfer of personal data to private parties in third countries outside of existing bilateral or mutual legal assistance agreements should, in principle, be prohibited. Following Article 5.3.i. of Recommendation No.R(87)15[30], the communication of data to a private party **based in the same country** should only be permissible if, in a particular case, there exists a clear legal obligation or authorization, or with the authorization of the supervisory authority. Nevertheless, Article 5.3.ii. of the same recommendation makes the transfer of personal data to private parties based in the same country **exceptionally permissible** if it is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent or it is necessary so as to prevent a serious and imminent danger. This is particularly important when the transfer is foreseen to private parties in third countries.

The WP29 therefore expresses concerns with regard to Article 36aa introduced by the Council as it would allow a broad transfer of data to third countries merely on the basis of the performance of the tasks of the competent authority and not in relation to public interest recognized by law. Derogations from the general transfer regime should not be based only on the performance of tasks, which may be defined broadly, but on the existence of important reasons of public interest.

[27] Everyone has the right to the protection of personal data concerning him or her.

[28] In this regard, the term 'adequate level of protection' must be understood as requiring the third country to ensure, by reason of its domestic law or its international commitments and by its practice/effectively, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union**.**

[29] In this regard, see Commission and EP versions of the text.

[30] Recommendation No.R(87)15 regulating the use of personal data in the police sector adopted by the Committee of Ministers of the Council of Europe on 17 September 1987 at the 410th meeting of the Ministers' Deputies.

Additionally, the use of the term "recipient" implies that data may be transferred to any public or private entity in the third country. Both elements contribute to the setting of a very low threshold for the application of a derogation that might entail the transfer of data to countries without an adequate level of protection and without any suitable safeguard. In this regard, the WP29 refers to its recent work on transborder access to data in cooperation with the Cybercrime committee of the Council of Europe[31].

The WP29 therefore recommends amending Article 36aa in order to clarify the hypothesis in which it could be used and reflect that the principle should be a prohibition and present the only exceptions allowed to it.

Ensuring consistency with Article 43A of the proposed Regulation

The WP29 insists that the text of the Directive be consistent with the proposed Regulation with regard to requests made by third country public authorities. Transparency should be ensured with regards to requests received.

12/ Role and powers of the supervisory authorities

The WP29 insists that text establishing the possibility for Member States to provide for an obligation to consult with the supervisory authority should be included in the text of the Directive. This would allow respecting national practices with regard to notifications.

In order to be effective, the Directive should provide efficient tools for data protection authorities. The power to suspend data processing, including, where relevant, suspension of data transfers to third countries, and to bring processing operations into compliance in a specified manner should be introduced in order for the supervisory authority to have sufficiently dissuasive, strong and effective powers. These are crucial to ensure compliance.

For the day to day supervision, particularly when carrying out inspections and imposing sanctions, DPAs need harmonized and effective investigative and sanctioning powers. As the Directive is meant to set minimum safeguards, the WP29 would favour a more detailed description of those powers in order to ensure consistency between supervisory authorities and to ensure that their authority is respected by data controllers.

Having in mind differences in national legal systems and given that mere access to information is not sufficient, WP29 recommends introducing the obligation for all Member States to provide their supervisory authority with investigative powers covering access to any data and documentation necessary for the performance of its tasks, means of processing and premises where data processing is being carried out. This should be done in compliance with Union law and/or Member State procedural law.

The WP29 therefore favours text on the powers of DPAs including effective investigative as well as corrective powers.

13/ Right to lodge a complaint

The WP29 supports the view that data subjects should be entitled to lodge a complaint, at least to the DPA, in the Member State where they have their habitual residence (Art. 50). It

should be for the European Data Protection Board to ensure the necessary cooperation of the DPAs of the Member States.

In this regard, the WP29 suggests ensuring consistency between the text of Article 50 and the text proposed by the Council for Article 73(1) of the draft regulation, i.e. : "Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a single supervisory authority, **in particular in the Member State of his or her habitual residence**, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her does not comply with this Regulation."

14/ Previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation

The issue of articulation of the directive with existing adequacy decisions and bilateral agreements concluded with third countries remains unsolved.

The WP29 is of the opinion that a review of the existing agreements is needed in order to ensure that such instruments are not used as a way to circumvent the rules laid down in the Directive as well as a way to ensure that the new data protection regime applies to all the personal data processing under its scope of application[32].

In this regard, while the draft proposal from 2012 entrusted competent authorities with the obligation to amend, where necessary, previously concluded international agreements within five years after the adoption of the Directive, the wording of the Council seems to avoid such review by stating that those agreements which are in compliance with Union law applicable prior to the entry into force of the Directive will remain in force until amended, replaced or revoked.

The WP29 therefore supports the proposal made by the Commission, and supported by the European Parliament, i.e. the introduction, in Article 60, of an obligation to amend, where necessary, previously concluded international agreements within five years after the adoption of the Directive. At the very least, it would favour ensuring that the existing instruments are applied in a way consistent with the Directive.

[32] In this regard, see also remark above made on Article 59.