ARTICLE 29 DATA PROTECTION WORKING PARTY

00530/12/EN
WP 191

Opinion 01/2012 on the data protection reform proposals

Adopted on 23 March 2012

Table of content

Introduction

The Article 29 Data Protection Working Party (Working Party or WP29) welcomes the proposals adopted by the European Commission that seek to reinforce the position of data subjects, to enhance the responsibility of controllers and to strengthen the position of supervisory authorities, both nationally and internationally. Subject to further improvement the rules proposed can significantly reduce the existing fragmentation and strengthen data protection across Europe.

The Working Party in particular welcomes the inclusion of provisions that give incentives to controllers to invest, from the start, in getting data protection right (such as data protection impact assessments, data protection by design and data protection by default). The proposals place clear responsibility and accountability on those processing personal data, throughout the information life cycle.

The Working Party underlines the importance of the provisions intended to clarify and strengthen data subjects' rights, notably by clarifying the notion of consent, the introduction of a general transparency principle and enhanced redress mechanisms. Also, the introduction of a data breach notification duty that provides consistency across all sectors is very welcome.

The Working Party also welcomes the fact that the proposals harmonise the powers and competences of supervisory authorities to more effectively ensure and where necessary enforce compliance, both individually and in cooperation with each other, for example, by being able to impose significant fines.

Despite its general positive stance toward the proposed Regulation, the Working Party feels that parts of the proposal for a Regulation need clarification and improvement. With regard to the Directive for data protection in the area of police and justice, the Working Party is disappointed by the Commission's level of ambition and underlines the need for stronger provisions.

The Working Party has carefully studied both proposals and with this opinion provides its first general reaction to them. The opinion highlights areas of concern and where appropriate makes suggestions for improvement. Where appropriate, the Working Party may produce further opinions on specific provisions or aspects of the proposals in the future.

The Working Party calls on the Council and members of the European Parliament to take the opportunity to improve both proposals and enhance the protection of personal data in the European Union.

General remarks

The Regulation fulfils the ambition to produce a text that reflects the increased importance of data protection in the EU legal order (Article 16 of Treaty, Article 8 of Charter). It retains and strengthens the core principles of data protection, imposes clear and uniform obligations on data controllers and processors, facilitates free movement of personal data and provides a strengthened legal framework for a uniform application of the law by Data Protection Authorities (DPAs) whose powers have been strengthened.

The Working Party is disappointed that its views on comprehensiveness have not resulted in one legal instrument. The Working Party notes the fact that the Commission has chosen to present a separate proposal for a Directive applicable to the area of police and criminal justice due to political constraints. A high level of consistent data protection standards also applying to this area is all the more needed. In any case, it should be clear that the new Directive must not result in Member States lowering their current data protection standards set for the police and criminal justice sector. Also, the new legal framework should be in line with other international agreements, including Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional protocol. The Working Party proposes to have a clear reference in the preamble of the Regulation and of the Directive to Convention 108 and its additional protocol.

In previous opinions, the Working Party has stressed the need for comprehensiveness to be achieved by the legal framework. From that point of view, the Directive is disappointing in its lack of ambition compared to the Regulation. The fact that two legal instruments have been presented does not necessarily mean that a comprehensive legal framework is no longer possible, as long as the goal is the same – to achieve a high level of data protection for the European citizen across the board – and that the instruments contain a common approach to, among others, the principles of data protection, data subject rights and the obligations for controllers and processors.

Serious efforts from the European legislator are needed during the legislative procedure to bring the substantive provisions of the Directive closer to those of the Regulation and to ensure consistency in both texts.

Furthermore, the EU institutions should be bound by the same rules that apply at Member State level. Therefore, for the reform to be truly comprehensive, at the moment when the Regulation enters into force, the framework for data protection for the European Union's institutions as currently laid down in Regulation 45/2001 needs to be aligned with it.

The same reasoning goes for the current specific rules for data processing in the former third pillar of the EU, for example in relation to EU agencies like Europol and Eurojust. The Working Party notes the practical difficulties that may exist to propose a general overhaul of the current acquis, but at the same time believes the same high level of data protection should in the end be applicable to all data processing in this area, including the EU bodies.

That said, the Working Party notes the commitment of the Commission to ensure a revision of other legal instruments to identify the need for alignment in three years. The Working Party recommends the legislator to set a much stricter deadline and calls upon the Commission to indeed put forward such proposals. At the same time the Working Party acknowledges that the current data protection regimes for some existing instruments and bodies are further-reaching than the proposed Directive. As is mentioned for Member States with a similar situation, alignment of current regimes with the Directive should in no case mean lowering a current data protection standard.

On another note, the Working Party regrets that neither the Regulation nor the Directive addresses the issue of the collection and transfer of data by private parties or non-law enforcement public authorities that are in fact intended for law enforcement purposes, as well as the subsequent use of these data by law enforcement authorities. Several examples in the last decade (i.e. PNR, retention of telecommunications data) have made clear that strict

conditions are needed, especially when such processing happens on a structural basis. The same applies the other way around: also rules are needed to ensure data protection when information is transferred from law enforcement or other "competent" authorities to the private sector or other public authorities.

Lastly, with regard to both proposed instruments, the Working Party notes with concern the extent to which the Commission is empowered to adopt delegated and implementing acts. While recognising the need to ensure that certain issues can be dealt with at a more detailed level at a later stage, the Working Party considers this is not the case, for example, for rules regarding data breach notifications. In order to ensure legal certainty essential elements should be inserted in the Regulation itself, as provided for by Article 290 TFEU.

With regard to the Regulation

Positive aspects

- In general, the Regulation provides greater clarity through more precise definitions and provisions aimed at ensuring a more harmonised application of the law, thus facilitating the free movement of data.

- For individuals the Regulation strengthens their rights including more transparency, greater control over processing, data minimisation, specific provisions for processing of childrens' personal data, strengthened right to data access, strengthened right to object, right to data portability, strengthened right to data deletion ("right to be forgotten") and strengthened right to redress both through the DPA and the courts.

- For data controllers the Regulation brings simplification and greater consistency, a strengthened focus on their accountability for data processed and the need to demonstrate this through data protection by design, data protection by default, privacy impact assessments, appointment of a DPO, data breach notification duties and the adoption of a precautionary approach to international transfers. In addition, Binding Corporate Rules are expressly recognised as a tool to frame international transfers.

- For data processors data security obligations are legally grounded and an obligation introduced to take on the responsibility of controller for a specific data processing operation if the processor goes beyond the instructions of a controller regarding that processing operation (relevant to 'cloud' providers).

- For DPAs the Regulation provides for strengthened independence and powers, including administrative fines and the obligation to be consulted on legislative measures, and provisions to ensure harmonised application and where necessary enforcement of the law, especially through the "consistency mechanism".

Role of the Commission

The Working Party has serious reservations with regard to the extent the Commission is empowered to adopt delegated and implementing acts, which is especially relevant because a fundamental right is at stake. Naturally, leaving certain issues to delegated and/or implementing acts may be necessary. However, not all issues referred to in Articles 86 and 87 are matters of detail. Some provisions of the Regulation (for example on data breach notification, mutual assistance, consistency and the exemption to the right of information and access in the context of processing for historical, statistical and scientific research purposes) cannot be applied without the delegated or implementing act being in place. In addition, other delegated acts concern the material scope of the Regulation, e.g. Article 6(1)(f) in conjunction with Article 6(5), which allows the Commission to define the "legitimate interests" of the controller in specific processing situations and sectors. In order to ensure legal certainty essential elements need to be inserted in the Regulation itself, as provided for by Article 290 TFEU.

In practice, the adoption of delegated or implementing acts for a large numbers of articles may take several years and could represent legal uncertainty for the controllers and processors which expect implementation and concrete guidelines rapidly. At the very least the Working Party calls on the Commission to set out which delegated and implementing acts it intends to adopt in the short, medium and long term.

Notwithstanding the role of the Commission as guardian of the Treaties, the Working Party also has strong reservations with regard to the role foreseen for the Commission in individual cases which have been dealt with under the consistency mechanism, as it encroaches upon the independent position of DPAs. When a matter is being dealt with or has been dealt with by the EDPB under the consistency mechanism, the Commission should be able to provide its legal assessment but should in principle refrain from interference. A procedure could be envisaged to enable the Commission and the EDPB to ask the European Court of Justice for an opinion on the interpretation of the Regulation.

Role of European Data Protection Authorities in policy making

The Working Party believes that the important role it has played until now and that the European Data Protection Board (EDPB) can play in the future in terms of policy making (for example by issuing guidelines or recommendations) should be reflected in the proposals.

In Article 66 it is stipulated that the EDPB shall on its own initiative, or at the request of the Commission, advise on any issue related to the protection of personal data and examine any question covering the application of the Regulation. The Working Party understands this as also including other legislation and therefore suggests to add in Article 66(1)(a) "*...and on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Union measures affecting such rights and freedoms*".

In addition, the Working Party suggests to create a possibility not only for the European Commission but also for the European Parliament to ask the EDPB for an opinion by adding "*and the European Parliament*" in Article 66(1)(b).

Furthermore, the Working Party strongly suggests to include an obligation for the Commission to in any case consult the EDPB on adequacy decisions (in Article 41) and on standard data protection clauses (in Article 42) and to consult and get approval from the EDPB on codes of conduct on a European level (in Article 38). An obligation for the Commission to consult the EDPB with regard to all delegated and implementing acts should in any event be included (in Articles 86 and 87).

National authorities should still be able to develop guidelines and recommendations which should be submitted to the consistency mechanism in case of significant impact on other Member States. They should also be able to monitor the development of certification seals and marks intended to protect individuals.

Thresholds for SMEs

The Working Party notes that throughout the proposal for a Regulation, exceptions and thresholds are introduced in order to limit administrative burden and alleviate the consequences for micro, small and medium size enterprises (MSMEs). Thresholds are introduced in the provisions regarding the obligation to designate a representative in the EU (Article 25), documentation (Article 28(4)), the appointment of DPOs (Article 35(1)) and the imposition of administrative fines (Article 79(3)). In addition the proposal provides for delegated and implementing acts allowing the Commission to take additional matters regarding MSMEs in Article 12(6) on procedures and mechanisms for exercising the rights of data subjects, Article 14(7) on the obligation to provide information to the data subject, Article 22(4) regarding accountability obligations and Article 33(6) on carrying out data protection impact assessments.

The Working Party is of the opinion that data subjects should have the same level of protection, regardless of whether their data is processed by a MSME or large-size enterprise. However, it recognises that some of the obligations proposed could be burdensome for MSMEs. Therefore, whilst the Working Party in principle recognises the reasons for introducing these thresholds, it fears the exceptions introduced may both in practice and in relation to the protection of personal data, lead to inconsistent outcomes and undesirable results. The Working Party believes that a threshold that takes into account the nature and extent of data processing would be more suitable.

Implications on budget and resources

The Working Party is pleased that the proposals recognise the important role DPAs can play in ensuring compliance by introducing enhanced duties for both DPAs and the EDPB. The Working Party does however have serious doubts as to whether the significant budgetary implications of these enhanced duties are sufficiently recognised. To empower DPAs and the EDPB to effectively carry out their duties, including mutual assistance and cooperation within the consistency mechanism, Member States must be committed to provide the necessary financial, human and technical resources.

In this respect the Working Party strongly suggests an independent in-depth assessment of the increased costs for DPAs and the EDPS (as secretariat for the EDPB) based on the current proposals, be carried out. Following the results of such an assessment, what constitutes ‘adequate human, technical and financial resources, premises and infrastructure’ for DPAs as mentioned in Article 47(5) should be made clear.

The Working Party intends to address the Commission regarding the purpose and parameters of such an impact assessment in a separate letter.

General provisions

Scope

According to Article 3(2) the Regulation also applies to processing of personal data of data subjects residing in the Union by a controller that is not established in the Union, where the processing activities are related to the offering of goods and service to such data subjects in the Union or the monitoring of their behaviour.

Notwithstanding attempts to define what is meant by both 'offering of goods and services' and 'monitoring of their behaviour' in the recitals, the Working Party feels further clarification of these notions would be helpful.

It should be made clear that the 'offering of goods and services' also includes free services (where individuals in fact pay for the service by providing their personal data). The Working Party therefore suggests adding wording along the lines **"***including services provided without financial costs to the individual"*.

Furthermore recital 21 implies that 'monitoring of behaviour' is linked to tracking on the internet and creating profiles. The Working Party advises to change the wording in order to ensure that even if the controller does not create profiles as such, processing activities can sometimes be considered 'monitoring of behaviour' if they lead to decisions concerning a data subject or involve analysing or predicting his or her personal preferences, behaviours and attitudes.

Data subject and personal data

The Working Party welcomes the definition on 'data subject' in Article 4(1) of the proposed Regulation, which states that a "*data subject means an identified natural person or a natural person who can be identified... "*. A natural person can be considered identifiable when, within a group of persons, he or she can be distinguished from the other members of the group and consequently be treated differently. This has been set out in the earlier adopted opinion of the Working Party on the concept of personal data (WP136). Recital 23 should therefore be amended in order to clarify that the notion of identifiability also includes singling out in this way.

Recital 24 relating to the definition of personal data foresees that identification numbers, location data, online identifiers or other specific factors need not necessarily be considered as personal data in all circumstances. As it stands now, the last sentence might lead to an unduly restrictive interpretation of the notion of personal data in relation for instance to IP addresses or cookie IDs. The Working Party recalls that personal data are data that relate to an identifiable individual. "*(A)data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated*"[1]. The Working Party has

[1] WP136, p. 10.

already developed in its opinion WP136 different scenarios which justify why IP addresses should be considered as relating to identifiable individuals, *'especially in those cases where the processing of IP addresses is carried out with the purpose of identifying the users of the computer (for instance, by Copyright holders in order to prosecute computer users for violation of intellectual property rights) (...)*'. In this case as well as in the case of cookies, the controller anticipates that "means likely reasonably to be used" will be available to identify the persons and treat that person in a specific way[2]. The Working Party therefore suggests changing recital 24 accordingly.

Biometric data

The Working Party welcomes the introduction of a definition of biometric data in Article 4(11) of the Regulation. Nevertheless, it has reservations about the current wording that focuses on allowing the unique identification of an individual. Biometric data are not just used for identification purposes, but also for the purpose of authentication (to verify the identity without actually identifying the individual). The definition should be amended to focus on what types of data are to be considered biometric data instead of focussing on what they allow. The Working Party therefore suggests to change the wording in Article 4(11) from *"...allow their unique identification..."* to *"...are unique for each individual specifically..."*.

Main establishment

The manner in which it is decided where a multinational company (whether EU-owned or non-EU-owned) has its main establishment, as defined in Article 4(13) and in recital 27 needs to be further clarified, including where it has separate legal entities operating in different sectors. For example, the 'dominant influence' of one establishment over processing operations with respect to the implementation of personal data protection rules could be taken into account.

The Working Party notes that the draft Regulation in Article 4 contains different definitions for business units, which are not clearly distinct from each other. The concepts of 'controller' and 'main establishment' on the one hand refer to where relevant decisions on data processing are taken, while – on the other hand – the definitions of 'enterprise' and 'group of undertakings' speak of the economic activity and the corporate structure.

An additional term is introduced with regard to processors, where the main establishment is supposed to be the place of the 'central administration'. Furthermore, Chapter VIII on remedies, liability and sanctions refers to any establishment when deciding the competent court in proceedings against a controller or a processor, regardless of whether this establishment has anything to do with the processing in question (it might indeed be legally completely independent from other EU establishments of the controller/processor).

In the Working Party's view, these definitions overlap and should therefore be further clarified. It should in any case be made clear what the link is between main establishment and the responsibilities of the controller.

[2] WP136, p. 16.

The definition of main establishment seems primarily intended to determine which national DPA should be the lead DPA in a particular case, or for a particular company. A clear understanding of the term 'main establishment' is crucial, as it is decisive for determining the lead authority in the meaning of Article 51(2), where processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State (see further on page 25).

Pseudonymisation

The Working Party believes that the concept of pseudonymisation should be introduced more explicitly in the instrument (for example by including a definition on pseudonymised data, consistent with the definition of personal data), as it can help to achieve better data protection, for example, in the context of data protection by design and default. The Working Party therefore suggests introducing a general obligation to anonymise or pseudonymise personal data where feasible and proportionate according to the purpose of processing. Such a principle could be introduced in Article 5 and in the context of data protection by design and default in Article 23.

Data protection by design and data protection by default

The Working Party welcomes the introduction of data protection by design and data protection by default in Article 23, but advises to further clarify its meaning in a recital, for example, by indicating that privacy friendly features of products and services should be activated automatically, and adequate procedures shall be implemented during the design of the data processing or a product. Naturally it is up to the controller to demonstrate that its processing activities take into account the concepts of data protection by design and data protection by default, which constitute appropriate measures in the context of Article 22(1).

The Working Party notes that the Commission is empowered to lay down technical standards in this area. The Working Party strongly believes that the Commission should involve and where appropriate consult the EDPB and international standardisation organisations when drawing up such technical standards.

<u>The principle of public access to information</u>

Recital 18 stipulates that the Regulation allows for the principle of public access to official documents to be taken into account when applying the provisions set out in the Regulation. As the principle of public access to official documents is a longstanding and important fundamental right, it should not only be mentioned in a recital but also expressed in an article of the Regulation.

<u>Further incompatible use</u>

Article 6(4) introduces the possibility of further processing of data for incompatible purposes in cases where another legal basis (except for legitimate interest of the controller) can be found. Whilst the Working Party does not question the need for leaving open possibilities for data to be further processed for other purposes, the provision as currently proposed opens up possibilities for further use of data for incompatible uses which could, both in the public and

private sector, especially if based on (b) (performance of a contract) and (e) (public interest), lead to highly undesirable results. In the view of the Working Party this provision runs counter to the general purpose limitation principle which is one of the key notions of data protection in Europe and therefore strongly suggests to either delete Article 6(4), or to redraft it in a more precise way with a reference to Article 21. In this context, the Working Party also wishes to draw the attention to the fact that it will address more substantially in an opinion the issue of compatible use in the course of 2012, as indicated in its Work Programme for 2012-2013.

Exceptions introduced for public authorities

One of the reasons for the revision of the data protection framework is to ensure comprehensiveness. By providing a single set of rules to be applied by both the public and private sector, the legal framework should enhance legal security and certainty with regard to the data protection safeguards offered across sectors, in particular for individuals.

The Working Party has already expressed its disappointment with regard to the lack of ambition in the area of police and justice. However, also within the Regulation itself a separate position is granted to the public sector. The Working Party is concerned that in several parts of the Regulation broad exceptions for public authorities are introduced for reasons of public interest. The Working Party believes that broad and unspecified exceptions, that also lack adequate safeguards for the protection of individuals, are unjustified. Therefore it suggests identifying within the Regulation as much as possible the specific public interests. This would also contribute to harmonisation within the EU.

As mentioned above Article 6(4) introduces a very broad possibility of changing the initial purpose of processing for incompatible purposes also for public authorities. In addition, Article 9(2)(g) allows for the processing of sensitive data for tasks carried out *"in the public interest"*. The same applies as to the exceptions laid down in Article 17(5), in particular with regard to the public interest and the interests of third parties. The Working Party advises to limit this exception to "*...for reasons of substantial public interest*".

Furthermore, Article 21 provides for the possibility of restrictions on data protection principles and data subjects' rights, hereby widening the possibility of restrictions compared to the current situation, without providing adequate safeguards that should be adhered to when the article is invoked. Furthermore, Article 21(1)(c) can be invoked to safeguard an open category of *"other public interests"* . The Working Party feels this is too broad and therefore strongly suggests to delete the phrase *"other public interests of the Union or of a Member State..."* in Article 21(1)(c) and start from *"...an important economic or financial interest..."*.

Article 33(5) introduces an exception for public authorities to the obligation to conduct data protection impact assessments (DPIAs) when processing results from a legal obligation. The Working Party is of the opinion that the only exception that could be justified in this context is when a data protection impact assessment has already been carried out in the legislative process.

The Working Party strongly believes general exceptions for the public sector are unjustified and are a detriment to the comprehensiveness of the legal framework and strongly suggests that, so far as is possible, the public and private sector are treated in the same way and are obliged to abide by the same set of basic rules. However, it must also be prevented that the

new legal framework might lead to a situation where the level of data protection already achieved in the Member States in different areas would be weakened. Particularly in the public sector, the level of data protection differs as a result of constitutional and legal traditions and developments. The new legal framework should therefore provide for a harmonised high level of standards in this area, while creating possibilities for Member States to provide for further specification (as already provided in Chapter IX), but without prejudice to the Regulation. This also means that they could supplement the Regulation.

Minors

The Working Party recognises the importance of the principle of "best interest of the child" and the notion of progressive protection in accordance with maturity level.[3] Whilst the Regulation does not interfere with the rules on the validity, formation or effect of a contract in relation to a child in Member States' general contract law, the Working Party welcomes that, in relation to the offering of information society services directed to a child, Article 8(1) regulates that the processing of personal data of a child below the age of 13 is only lawful if and to the extent that consent is given or authorised by a child's parent or custodian.

The Working Party is mindful of the constraints in harmonising age limits in such an instrument and understands that in cases that are purely national, Member State law should apply. The Working Party would however suggest broadening the scope of the minimum rule introduced in the Regulation with regard to the manner in which minors are treated to other issues, besides offering of information society services, as there are more situations in which specific rules could be envisaged.

In general, the Regulation lacks provisions with regard to the manner in which rights can be executed by representation, not only in the case of minors, but also in case of representation for incapable persons and by lawyers.

Right to be forgotten

The Working Party welcomes the specific inclusion of the right to be forgotten and to erasure in the Regulation as a means to strengthen the control that individuals have over their personal data. However, the way in which these rights are configured by the Regulation and the reality of how the internet works may significantly limit their effectiveness.

The controller is responsible not only for the erasure of data but also for informing third parties that are processing this data by means of links, copies or replications of the request of the data subject. Placing this obligation only on the controller has limitations, as there may be cases where the controller has taken all reasonable steps to inform third parties, but is not aware of all existing copies or replications or when new copies or replications appear once the controller has informed all known third parties. More importantly, no provision in the Regulation seems to make it mandatory for third parties to comply with the data subject's request, unless they are also considered as controllers.

[3] See Opinion 2/2009 on the protection of children's personal data (WP 160) and Working Document 1/2008 on the protection of Children's Personal Data (WP 147)

The Regulation gives no direction on how data subjects can exercise their rights if the controller no longer exists, has disappeared or cannot be identified or contacted. Therefore, the position of third parties that process data should be clarified in order to define the terms and capacity in which they are to follow the data subject's request, and the consequences of not doing so.

Along the same lines, consideration could be given to extend the right of data subjects to allow them to directly address requests for erasure to third parties in cases where that cannot be done through the controller.

Finally, there is no mechanism that provides for the deletion of links to, copies or replications of data which is not erased in line with Article 17(3), but which in itself do not fall under the grounds of the article. Such links, copies or replications however may facilitate access to the original content while this might not necessarily be justified under said article. Naturally, the Working Party recognizes the need to balance privacy rights against the right to freedom of expression. The Regulation should clarify the relation between Article 17(3) and the obligation in Article 17(2).

Direct marketing

Notwithstanding Article 19(2) of the Regulation which provides for a right to object to data processing for direct marketing purposes, the Working Party underlines that the provisions of Directive 2002/58/EC remain fully applicable, as is also provided for in Article 89 of the Regulation. This specifically applies in the context of online behavioural advertising and e-mail marketing, where consent is foreseen.

Profiling

The Working Party supports the provision in the Regulation dealing with profiling. However, it has doubts whether the approach taken is sufficient to reflect the issues of creating and using profiles, particularly in the online environment. In addition, the Working Party notes that the term “significantly affects” in Article 20(1) is imprecise. It should be clarified that it also covers the application of, for example, web analysing tools, tracking for assessing user behaviour, the creation of motion profiles by mobile applications, or the creation of personal profiles by social networks.

Furthermore, the provision should not be limited to solely automated processing but should also cover partly automated processing methods. In the Working Party’s view, an approach should be taken that clearly defines the purposes for which profiles may be created and used, including specific obligations on controllers to inform the data subject, in particular on his or her right to object to the creation and the use of profiles.

Representative

The Working Party believes the role and obligations of the representative as stipulated in Article 25 should be further clarified. It should be made clear what role the representative has vis-à-vis data subjects, courts and DPAs, especially considering the fact that Article 79(6)(f) provides for the highest possible fine in case of failure to designate a representative. It should be specified what the mandate of the representative is in order to clearly determine the scope of its mission, role and liability.

Article 78(2) stipulates that where the controller has designated a representative, any penalties shall be applied to the representative. The same clarity should be provided in the case of administrative sanctions according to Article 79. The wording *"may be addressed by the supervisory authority"* used both in recital 63 and in Article 4(14) does not sufficiently make clear that a representative can also be the addressee of an administrative sanction in the meaning of Article 79.

It should also be clear that the establishment of a representative in the EU as stipulated in Article 25(3) *"shall be established in one of those Member States"* does **not** trigger the main establishment mechanism as stipulated in Article 4(13) in the sense that it does **not** play a **decisive** role in determining a lead DPA from Article 51(2).

With regard to the exceptions to the obligation to designate a representative, the Working Party does not see any substantial reason to exclude a controller from a third country offering an adequate level of protection. The fact that a third country has an adequate level of data protection does not alter the need to have a contact point in the European Union and the Working Party therefore suggests to delete Article 25(2)(a).

If exceptions to the obligation to designate a representative are to be introduced, they should be based on the nature and extent of personal data processing, as well as the (potential) number of affected data subjects in the EU. The current threshold of the amount of persons employed by the controller risks excluding small organisations carrying out processing that pose risks to individuals. Also, notwithstanding the explanation in recital 64 the wording "***only occasionally*** *offering goods or services to data subjects*" is too vague and could in practice too often lead to misinterpretation.

Accountability

The Working Party very much welcomes the introduction of the principle of accountability in the Regulation, especially in Article 22, and strongly agrees with the aim to put in place effective procedures and mechanisms which focus on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects. Nonetheless, the Working Party has some doubts about the articles that seek to specify the general principle.

First of all, scalability must be ensured. In implementing the principle of accountability, it should be possible to take into account the size of the controller and the nature of the processing activities. Furthermore, the supervisory authorities should be enabled to consider the implemented accountability mechanisms, when issuing sanctions and fines.

In addition, Article 28 provides for an obligation for the controller to maintain documentation of all processing operations taking place under its responsibility. Article 28(2) prescribes which specific documentation this entails. This obligation interacts with the general obligations to be accountable in Article 22, where controllers are obliged to *be able to demonstrate* which policies are adopted and measures implemented to ensure compliance. In principal, each controller, processor and, if any, the controller's representative should be obliged to keep core documentation on its data processing operations.

While the Working Party welcomes the obligation of carrying out a data protection impact assessment as provided for in Article 33, it feels that carrying out an impact assessment should naturally be done also when it is not clear whether the processing would present specific risks to the rights and freedoms of data subjects. Therefore the Working Party suggests to bring Article 33(1) in line with recital 70 and proposes to add "*are likely to*", so that the first sentence of the article reads "*Where processing operations **are likely to** present specific risks...*".

The Working Party considers that the exemptions provided for in Articles 28(4)(b) on documentation and 35(1)(b) on the appointment of DPOs may have unintended consequences, especially where a small organisation with less than 250 employees processes a lot of personal data or the processing is risky by nature. Equally, the current wording disproportionately affects large organisations processing limited personal data. The Working Party feels that instead of the total number of employees of a company it would be more suitable to take into account the nature and extent of personal data processing, as well as the numbers of staff directly involved in processing personal data and/or the number of data subjects.

The Working Party believes that processing activities regarding the categories of sensitive data as in Article 9 of the Regulation, should be submitted to a data protection impact assessment. Therefore all elements of sensitive data should be taken on board in Article 33(2)(b).

In addition, the limitation of processing operations under Article 33(b, c & d) to processing *"on a large scale"* should be deleted, as the Working Party believes that a data protection impact assessment is required for such processing operations even on a small scale.

This is especially true for the processing of biometric data, which the Working Party feels under certain circumstances should be considered risky and therefore a data protection impact assessment should be carried out irrespective of any thresholds provided for in Article 33. Also, as mentioned earlier, the exception for public authorities in Article 33(5) to carry out an impact assessment is unjustified, unless such an assessment has already been carried out during the legislative process.

Data breach notification

The Working Party welcomes the introduction of the duty of the notification of a personal data breach that provides consistency across all sectors. The Working Party nevertheless has doubts as to whether the way in which the notification duty is set up will lead to satisfactory results. Notably the scope of the duty to notify to the supervisory authority should be more focused and restricted. The situation that supervisory authorities are distracted by and overburdened with the processing of notifications of minor data breaches which are unlikely to adversely affect the rights of data subjects should be avoided. Furthermore, the role and responsibilities of DPAs in case of (and after) notification need to be clarified.

The Working Party is mindful of the fact that a 24-hour limit for notification could under certain circumstances not be feasible. In Article 31(1), this has been addressed by providing an opportunity to notify later than 24 hours after having become aware of the breach. Timely notification is nevertheless important. The Working Party therefore proposes to apply a two-step approach, whereby notification of the breach by the controller must in principle take

place within 24 hours after having become aware of the breach. In case all information cannot be provided within the 24 hour limit, the controller will have the opportunity to complete the notification in a second phase.

Further specification is needed regarding the criteria for establishing a personal data breach and the circumstances under which a breach must be notified to the DPA and the data subjects concerned (for example if there is a risk of concrete danger or damage for data subjects). The Working Party believes that the EDPB should in any case be involved in determining these criteria and circumstances.

In order to reflect recommendations by the Working Party and ENISA, the notification form should contain an evaluation of the severity of the breach of personal data based on objective criteria.

With regard to the role and functioning of DPAs

Independence

The current text states that members of the DPA can only be appointed by parliament or government. However, the Working Party wishes to allow for Member States to allow the possibility for other independent bodies, such as the Council for the Judiciary, to nominate and / or appoint members of the DPA as well.

Powers

In addition to the possibility of DPAs to carry out investigations, they should also have the explicit possibility to carry out audits.

Budget

For the effective performance of the enhanced duties and powers of DPAs by the Regulation, including those to be carried out in the context of mutual assistance, cooperation and participation in the EDPB, the Regulation stipulates that Members States need to ensure adequate human, technical and financial resources, premises and infrastructure for DPAs. As mentioned earlier, the Working Party strongly advises to more concretely indicate what amounts to an adequate budget, for example after an independent in-depth assessment of the increased costs for DPAs based on the current proposals has been carried out.

An adequate budget could be based on a fixed amount to cover the basic functions that all DPAs have to undertake equally, supplemented by an amount based on a formula related to the population of a Member State and its GDP. There might also be an element to reflect the number of multinationals that have their headquarters established in that Member State. One of the recitals should explicitly encourage Member States to consider a variety of options for funding the DPA, so as to ensure it can meet the requirement of an adequately resourced authority.

Margin of discretion

DPAs should be enabled to be selective in order to be effective; they should be able to define their own priorities and to start actions, such as investigations, on their own initiative, notwithstanding the obligations regarding cooperation, mutual assistance and consistency according to Chapter VII. DPAs should be able to allocate resources according to the strategic character and the complexity of issues at stake, for example by taking into account the actual or potential detriment to data protection, the number of persons concerned and the technology used. Allowing DPAs to set their own priorities also helps to deal with financial and budgetary constraints.

The duties under Article 52(2) and (3) which state that DPAs *"shall promote"* and *"shall, upon request, advise any data subject"*, seem to decrease the margin of discretion necessary for DPAs to be effective. Furthermore, in order to enable DPAs to have discretion the Working Party suggests including the word *"may"* in Article 34(3) as follows *"and **may** make appropriate proposals to remedy such incompliance"*.

Jurisdiction and competence of DPAs (one-stop shop)

Article 51(1) provides for the competence of a DPA on the territory of its own Member State. This general rule is complemented by Article 51(2) which states that the DPA of the Member State where a controller has its main establishment is deemed the DPA competent for the supervision of processing activities in all Member States.

The Article 29 Working Party is in favour of creating the concept of a lead authority and a clear obligation for DPAs to cooperate and to refer to the consistency mechanism in cases where data subjects in several Member States are likely to be affected by processing operations, as it will lead to a consistent interpretation and application of the EU legal framework, thus creating legal certainty. However, as mentioned above, in order for the mechanism to be able to function, the definition of main establishment and the consequences on the competences of other DPAs need to be clarified. Also the manner in which the consistency mechanism has been proposed raises questions.

It should in any event be clear that the competence of a lead DPA is non-exclusive. The competence of the lead DPA is subject to the obligations to cooperate, provide and accept mutual assistance, and make use of the consistency mechanism, as stipulated in Chapter VII on consistency and cooperation, and act in agreement with other involved DPAs.

Furthermore the Working Party stresses that the one-stop shop principle in Article 51(2) applies only to the situation where the controller or processor has more than one establishment within the EU, it does not apply to the situation where there is no establishment in the EU and where the processing activities are related to the offering of good and services to data subjects in the Union or the monitoring of their behaviour, according to Article 3(2). Consequently, in this case, any DPA whose Member State is affected by processing operations is competent according to Article 51(1), but the Regulation lacks rules on which DPA in these cases should be the 'lead'. The Working Party considers that cooperation and consistency are especially important in these cases.

Given that the current elements for defining main establishment in Article 4(13) are, as explained earlier, not satisfactory, and therefore there is a lack of clarity in establishing the lead competent DPA in cross-border cases, the Working Party proposes considering;

1. to accept the competence of a lead DPA to be non–exclusive, but subject to the obligations to cooperate, provide and accept mutual assistance, and make use of the consistency mechanism, as stipulated in Chapter VII on consistency and cooperation; and
2. in cases where there is no establishment in the EU (or it is unclear where the main establishment is) criteria for determining the lead DPA which could include:
    - the Member State in which the main processing activities in question are taking place;
    - the Member State in which individuals are affected;
    - the Member State in which individuals have specifically complained to or raised concerns with the DPA, according to Article 73(1).

It is clear that there may be several Member States for any of the abovementioned criteria. However, on the basis of these criteria the relevant DPAs should agree amongst themselves who should take on the responsibility of being lead. In cases where it is not obvious, or where there is no agreement, the EDPB should decide upon the lead, based on the same criteria.

Mutual assistance

The Working Party suggests a comprehensive concept of lead DPA and cooperation. Whenever, in the meaning of Article 56, *"data subjects in several Member States are likely to be affected by processing operations"*, there should be a general obligation for the respective DPAs to cooperate as their citizens are impacted. This cooperation should comprise the legal assessment as well as specific supervisory measures to be taken.

Following Article 55(1) the Working Party feels that DPAs should inform each other of other relevant information, also in cases where a measure as referred to in Article 58(1) has not yet been taken (for example in case of a security breach). In addition, DPAs should share amongst themselves favourable decisions taken on data protection impact assessments.

The Working Party suggests to clarify in Articles 55 and 56 that whenever a decision must be taken that involves both the lead DPA in the meaning of Article 51(2) and another concerned DPA according to Article 51(1), the lead DPA and the national 'on-site' DPA should act *in agreement* regarding the assessment of the case and of the measures to be taken. Where the concerned DPAs do not reach consensus on the assessment of the case and/or measures to be taken on a bilateral or multilateral basis, the case should be submitted to the consistency mechanism as in Article 57.

The Working Party welcomes the measures proposed to ensure DPAs can work together and notes that the competence of the lead DPA as discussed above is not exclusive. The Working Party stresses however that more is necessary to ensure mutual assistance, in terms of budget for DPAs as mentioned above, but also in terms of addressing important details of the manner in which mutual assistance is to be put to practice. The use of language, deadlines, the amount and nature of information requested as well as technical means, formats and procedures for information sharing, are all issues that in practice are vital to ensure effective cooperation between DPAs and therefore also stand at the core of the "one-stop shop" principle.

Consistency

The Working Party is pleased to note that its proposal for a mechanism for cooperation and coordination which is intended to ensure consistency of application of the rules on data protection is included in Articles 57 and 58 of the proposal.

The Working Party believes however that such a mechanism should ensure consistency in matters only there where it is necessary, should not encroach upon the independence of national supervisory authorities and should leave the responsibilities of the different actors where they belong.

Given the broad scope of Article 58(2)(a) covering data processing in the context of any sort of cross-border offering of goods or services within the EU, the Working Party suggests that only those cases should be subject to the consistency mechanism within the EDPB where the competent DPAs according to Article 51 do not reach consensus on the assessment of the case and/or measures to be taken on a bilateral or multilateral basis. In any event the EDPB should be informed of cases which are of general relevance for data protection or the free movement of personal data within the EU.

In order to avoid that a great number of cases could be triggered due to the fact that the scope of the mechanism is considerably broad (following Article 58(3) that states that **any** authority can request that any matter shall be dealt with in the consistency mechanism), the Working Party suggests to submit to a vote within the EDPB for requests submitted under Article 58(3).

Notwithstanding the role of the Commission as guardian of the Treaties, the Working Party has strong reservations with regard to the role foreseen for the Commission with respect to individual cases pending in the consistency mechanism, as it encroaches upon the independent position of DPAs and the EDPB. When a matter is being dealt with or has been dealt with by the EDPB under the consistency mechanism, the Commission should be able to provide its legal assessment but should in principle refrain from interference. This is particularly true in case of suspension of a measure as stipulated in Article 60(1), 62(1)(a) and (2). Moreover, “serious doubts” is not sufficient to trigger interference by the Commission.

The Working Party stresses that it is up to the EDPB itself to ensure that its opinions are respected and applied in a uniform manner by all relevant DPAs.

In order to increase the effectiveness of the opinions of the EDPB, a ‘confirmation mechanism’ could be introduced in cases where one or more DPAs intend to derogate from an opinion taken by the EDPB under the consistency mechanism according to Article 58(7). The EDPB should in those cases be able to re-confirm its opinion by qualified majority thus underlining the importance of a common approach in cases of general relevance for data protection within the EU. Another option would be to allow the possibility for DPAs to express minority positions. These positions should be motivated and made public.

In addition, a procedure should be envisaged to enable the EDPB and the Commission to ask the European Court of Justice for an opinion on the interpretation of the Regulation, if a DPA intends not to follow an opinion, which the EDPB has re-confirmed by qualified majority.

Application of national law (Chapter IX)

When specific rules are adopted in Member States under Articles 80-83, these rules will interact with the rules regarding the competence of DPAs and the system of lead DPA.

The text as it stands now does not solve the issue of cases arising out of adjacent national law, for example in the context of employment, in relation to the scope of competence of the DPA of the main establishment of the controller. The question is whether for example the German DPA would need to interpret and apply Spanish labour law in case of an issue regarding an employee of a subsidiary in Spain of a company with its main establishment in Germany. It should therefore be clarified that, as an exception to Article 51(2), in cases which depend on the application of national law according to Chapter IX of the Regulation the respective national DPA should always (naturally acting in cooperation with the lead DPA) be the competent one for applying adjacent national law in that specific case (in the example above the Spanish DPA would be competent to apply the specific Spanish data protection law in the context of employment).

In general, the Working Party stresses the need to clarify the scope of application of the national laws adopted under Chapter IX.

Deadlines

The Working Party agrees that timeliness of EDPB opinions sought through the consistency mechanism is important. The timeframe allocated to achieve results should however be such that the quality of the advice is guaranteed. In order to ensure the actual bearing and support on the ground and to ensure the advice can be upheld in possible court proceedings, the stringent timeframe proposed will in any event need to be extended.

<u>"One-stop shop" for data subjects</u>

Like data controllers, also data subjects within the jurisdiction of EU DPAs should have a "one-stop shop". In the Regulation there are several possibilities for data subjects to exercise their rights and seek justice. Data subjects can lodge a complaint with a DPA in all Member States (with their national DPA, the DPA of the Member State where the controller has its main establishment or any other DPA in the Union). Data subjects can also initiate proceedings before their national court and before the court of the country where the data controller has an establishment.

Although these possibilities might seem to enhance data subjects' rights, it might also lead to confusion and uncertainty as to whom will ultimately be responsible for providing an answer to the data subject.

Notwithstanding the right to a judicial remedy, the Working Party suggests to clarify that data subjects shall in principle address the DPA within the jurisdiction where they reside or the DPA where the data controller or processor has an establishment. In order to be able to respond to the data subject, the addressed DPA in this Member State would have to cooperate with the DPA of the main establishment of the controller (the lead DPA) in order to agree on necessary measures to investigate and in certain cases to take enforcement action. The DPA initially addressed will however in all circumstances remain responsible for responding to the data subject.

EDPB institutional structure

The Working Party notes that it will be replaced by the European Data Protection Board (EDPB) which is set up in Article 64.

The Working Party believes it should be able to democratically choose its own chair and vice-chairs. In the view of the Working Party no convincing reasons have been put forward to require the EDPS to be a permanent vice-chair.

In addition, the desirable option would be to have a completely independent secretariat. However, the Working Party notes that the secretariat of the EDPB is to be provided by the EDPS and no longer by the Commission. Further consideration should be given to how this can be achieved in terms of practical arrangements and reporting lines, in particular the need to ensure independence of the members of the secretariat and the legal and institutional consequences of entrusting the secretariat of the EDPB to one of its members.

International transfers

The Regulation rightly emphasises the accountability of data controllers to ensure that personal data remains protected when transferred outside of the European Economic Area (EEA). It facilitates data controllers by providing various "safe harbours" in the form of adequacy decisions, a streamlined system of BCRs for multinationals, approved contractual clauses and individual DPA approval. It also provides for various derogations in Article 44.

However, the scope of the derogations, especially Article 44(1)(h) remains very wide and tends to be applicable to many situations. According to the previous opinion of the Working Party (WP 114), such derogations should be applicable solely to the extent that the processing is not massive, not repetitive and not structural.

In addition, Article 42 introduces the possibility to use non binding instruments to frame international transfers, which are subject to authorisation from DPAs. Nevertheless, bindingness has always been considered as an important requirement in existing tools framing international transfers (for example CCT, BCR, SH, adequacy of third countries). Therefore, it is proposed to delete Article 42(5), except for the last sentence. Consequently, the reference in Article 34 needs to be adjusted accordingly.

Concerning Article 41(6) it should be clarified that whether *"without prejudice to Article 42 to 44"* means that in case of a negative adequacy decision of the Commission, data transfers to the concerned third country are nevertheless possible on the basis of all these articles.
Finally, where the Commission has decided that a third country or territory, or a processing sector within in that third country or international organisation in question ensures an adequate level of protection (Article 41), such transfer shall not require any further authorisation. However, as mentioned before, the Working Party strongly suggests including an obligation for the Commission to consult the EDPB on adequacy decisions.

Disclosures not authorised by EU law

The Working Party stresses the need to include in the Regulation the obligatory use of Mutual Legal Assistance Treaties (MLATs) in case of disclosures not authorised by Union or Member States law. The Working Party feels that without a provision on the obligatory use of MLATs when they are in place will, amongst others, allow for wide transfers of personal data for a large and unlimited category of *"important grounds of public interests"*, following Article 44(1)(d), including when these transfers have a massive, frequent and structural character. When a judgement of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to transfer data from the EU to that third country and there is no MLAT or another international agreement in force between the requesting third country and the Union or Member State(s), the transfer of such data should be prohibited. The Working Party underlines that in cases where a MLAT is in place, the competent authority under the MLAT (or comparable international agreement) shall be the authority dealing with the request and should, where necessary, consult the DPA.

Right to liability and compensation

The Working Party welcomes the provisions introduced in Article 77(1) to ensure any person who has suffered damage as a result of an unlawful processing operation or an action incompatible with the Regulation has the right to receive compensation by the controller or processor for the damage suffered. The Working Party also welcomes the fact that Article 77(2) ensures that the data subject does not bear the burden of addressing the responsible controller in case more than one controller or processor is involved in the processing. The Working Party considers however that it is necessary to clarify (in a recital) that the word "damage" does not merely mean material harm but also includes distress (harm that is not material).

If there is a decision taken by another DPA, (for example, the DPA of the main establishment) affecting or producing a prejudice to the data subject, the latter should be able to bring action against this decision before the administrative courts of her/his country of residence.

The solution as proposed by the European Commission, to have either the data subject or the DPA to bring action against the other DPA on the territory of this DPA is far from satisfactory. The Working Party calls for a system that allows data subjects to bring action against an administrative decision before the administrative court of their country of residence.

Fines

The Working Party welcomes the introduction of significant fines as these will enable DPAs to take up their role as enforcement authorities and can - as a deterrent - contribute to a higher degree of compliance by data controllers.

Article 79(1) provides that each supervisory authority "*shall be empowered*" to impose administrative sanctions. Recital 120 supports this by stating that the supervisory authority "*should have the power*" to sanction administrative offences. However Article 79(4 - 6) state that the supervisory authority "*shall impose a fine*" in the situations described. The Working

Party is of the opinion that DPAs should have a margin of discretion in deciding when to impose a fine, since many factors influence the nature of the infringement and should be taken into account when deciding on the imposition of a fine. It therefore suggests amending the wording in Article 79(4 - 6) accordingly.

The Working Party appreciates the harmonising effect of Article 79, which regulates what infringement leads to which maximum fine, as it will lead to more consistency in imposing fines across the European Union. Nonetheless, the Working Party suggests making explicit in Article 58(2) the possibility of using the consistency mechanism of section 2, Chapter VII to cover divergences in the application of administrative sanctions, as is also stipulated in recital 120.

The Working Party furthermore understands that where several DPAs are competent, they are all empowered to impose a fine following Article 79 of the Regulation. This does however raise questions with regard to the principle of double jeopardy (ne bis in idem).

Furthermore, the Working Party believes the threshold introduced in case of first and non-intentional compliance would in practice lead to many controllers falling outside of its scope and therefore feels the threshold should be deleted. If a threshold were to be introduced, it would in any case be more suitable to take into account the number of (negatively) affected data subjects than the amount of employees of the controller.

Judicial remedies

The Working Party welcomes the inclusion of a comprehensive set of rules on judicial remedies for data subjects, including the possibility for organisations or associations to exercise the rights of data subjects vis-à-vis data controllers and processors. However, in the Working Party's view, several aspects regarding Chapter VIII need further clarification.

Given the broad scope of Article 73(1), according to which every data subject shall have the right to lodge a complaint with a DPA in **any** Member State, the Working Party feels that the data subject should in principle address the DPA within the jurisdiction where they reside or the DPA in the jurisdiction where the controller or processor is located, as is also stated above under one-stop shop for data subjects.

Furthermore, when the DPA receiving the complaint seems not to be the right one on the merits of the case, the Working Party feels there should be an obligation for the receiving DPA to cooperate with the one-stop shop DPA of the data subject and the DPA where the controller is located. In this case, the DPA where the complaint was lodged should be obliged to inform the data subject on the progress of the case, regardless of whether or not it is competent on the merits of the case or not. This follows from the necessity of a one-stop shop for data subjects (see above).

With regard to Article 74(2) the Working Party feels it should be clarified which DPA should be competent to *"act on a complaint in the absence of a decision necessary to protect their rights"*. In the case of the lead DPA according to Article 51(2) this would be the DPA of the Member State where the processor/controller has its main establishment and in any other case this would be the competent authority according to Article 51(1). It should therefore be clarified in Article 74(2) that the obligation to act refers to the competent supervisory authority *"...in the meaning of Article 51(1) or (2)"*.

In addition, Article 74(4) provides that a data subject who is concerned by a decision of a DPA in another Member State than where it has its habitual residence, may request the DPA of the Member State where it has habitual residence to bring proceedings against the DPA in the other Member State. While the Working Party appreciates the reason for introducing such a provision to ensure data subjects can exercise their rights vis-a-vis a DPA in another Member State, it nevertheless considers it to be contrary to the general obligation for DPAs to cooperate and to provide mutual assistance in cross-border cases, according to Articles 55 and 56, and the fact that in cases where there is disagreement between DPAs the matter should be brought before the EDPB. Therefore the Working Party stresses the need to carefully consider alternatives for data subjects to get judicial redress against a decision of DPAs that affect them, that are consistent with the principles of the Regulation.

Article 75(2) provides for the possibility for data subjects to bring proceedings against a controller or a processor before the courts of the Member State where the controller or processor has an establishment or alternatively, such proceedings may be brought before the courts of the Member State where the data subject has habitual residence. The Working Party feels that the possibility to bring proceedings before the courts in **any** Member State where the controller or processor has an establishment, regardless of whether this is the main establishment or the establishment where the relevant decisions on data processing are taken, can be problematic.

Despite Article 75(4) which states that Members States shall enforce final decisions by other courts, it is doubtful whether a decision of a court in a Member State where the controller or processor does not have its main establishment, is truly enforceable. This needs to be clarified.

Furthermore, even though the Working Party welcomes the inclusion in Article 75(2) of the possibility to bring proceedings against a data controller before the courts of the Member State where the data subject has its habitual residence, which is similar to the concept of consumer protection according to the Brussels-I-Regulation and aims at strengthening the position of data subjects, it is unclear how the judgement of a court of the Member State where the data subject has its habitual residence, shall be enforced if the controller or processor is established in another Member State.

Both Articles 74(5) and 75(4) stipulate that Member States shall enforce final decisions by the courts referred to in these Articles. Such provisions are comparable to similar obligations in Article 111 of the Schengen Implementing Agreement. As mentioned, it appears to be unclear according to which procedural rules and by which national authorities decisions by courts of one Member State shall be enforced in another Member State. Furthermore, with regard to what constitutes “final” decisions, there might also be need for further harmonisation (Schengen Information System - case between AU and FR).

<u>Churches and religious associations</u>

The Working Party understands that Article 85 obliges churches and religious organisations that currently have separate legal regimes, to bring it in line with the Regulation. It shall in any case not grant churches and religious organisations the possibility to adopt a separate legal regime that is incompatible with the Regulation in those Member States where constitutional arrangements do not permit this.

With regard to the Directive

Choice of instrument

The Working Party notes the explicit choice of the European Commission not to present one single instrument for data protection across the board, and to present a Directive as the instrument to regulate data protection in the area of police and criminal justice at the high, consistent level of data protection it is aiming for. However, the Working Party also notes that the current proposal would result in lowering the data protection standards in several Member States. The Working Party finds this to be unacceptable and therefore calls on the European legislator to ensure that the current, higher data protection safeguards in the European Union are to be considered as the bare minimum for the proposed Directive. The Directive should not be construed in order to justify the striking down of additional data protection safeguards in the current laws of the Member States.

Consistency

Despite the different instruments proposed, the 'core' aspects of the provisions should be consistent, in particular as regards the principles, obligations and responsibilities, individual rights and powers and tools available to supervisory authorities. Indeed, given the sensitivity of the processing covered by the Directive, it would be unacceptable to have lower standards applying to this area. Of course, providing limitations and exceptions is necessary, notably concerning the rights of data subjects, but it must be made clear that these are exceptions and that the 'core' aspects are the same.

Scope of application

The Working Party notes and welcomes that the Directive has given up the distinction between the processing of personal data in domestic and in cross-border cases that was provided for under Framework Decision 2008/977/JHA. This limitation of the applicability of European legislation to strict cross-border cases has in the past been criticised by the Working Party.

The scope of application of the Directive should be as clear as possible. However, the text proposed raises various questions, among which are the following.

The Working Party notes the difficulty of separating the scope of application of the Directive from the scope of application of the Regulation. The Directive does apply if competent authorities process personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Under all other circumstances, the Regulation as the general instrument for the protection of personal data applies. However, account should be taken of the different traditions in the Member States to define the activities of their authorities as related to law enforcement purposes or merely administrative (for example, in the areas of customs, immigration, environmental affairs). In consequence, both instruments, the Directive and the Regulation, might apply to the same institution. Situations must be avoided where the same data processing operation, such as in relation to maintaining public order, in one country is covered by the Regulation, where in other Member States the laws based on the Directive apply. This is particularly troublesome if

both instruments lack consistency, as is currently the case. From this point of view more consistency between the two instruments is needed and more clarity with respect to the definition of "competent authorities" would be necessary. The Working Party considers that it must be clear to which activities vested in competent authorities by law the Directive applies.

The Working Party is of the opinion that it must be further clarified to what extent the Directive applies to the area of criminal procedure. The Working Party notes that the Directive applies to the processing of data for the purpose of prosecuting crimes (Article 1). At the same time, the Working Party understands Article 17 (and recital 82) to mean that Member States can decide to not align their national rules on criminal procedure with the rights as provided under Articles 11-16, at least in those cases where judicial procedures are concerned. Differences in national criminal procedure, however, make it difficult to determine what phase of the prosecution is referred to when the Directive, in Article 17, speaks about "national rules on judicial proceedings where personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings". The Working Party invites the European legislator to ensure no doubt can exist that the Directive applies to criminal procedures and the prosecution of crimes, also to avoid situations that no data protection would be offered as soon as a prosecutor or investigative judge is involved in a law enforcement operation or investigation, in line with Council of Europe Convention 108. Furthermore, the Working Party feels Article 44(2) needs clarification on the meaning and intention of the wording "to act in a judicial capacity". It should be clear what the relation between the DPA and the courts should be and under what circumstances supervisory tasks can be carried out.

Data processing principles

With regard to the principles, the Directive fails to include important elements regarding the retention of personal data (including retention periods), transparency towards individuals, keeping personal data up to date, and ensuring it is adequate, relevant and not excessive. Accountability provisions requiring the data controller to demonstrate compliance are also missing. The wording of Article 4 should be made consistent with the wording in the Regulation (Article 5).

The Working Party furthermore suggests including provisions limiting access to data to duly authorised staff in competent authorities who need them for the performance of their tasks.

In addition to the comments made above regarding a lack of consistency with the Regulation, the Working Party welcomes the distinction that is proposed to several categories of data subjects to be processed. It notes in particular a distinction that is to be made between data regarding suspects, victims, witnesses, etc. Also, it welcomes the distinction that has to be made based on the quality and accuracy of the data processed by the law enforcement authorities. The Working Party however regrets that these distinctions have been limited by adding the words "as far as possible" in Articles 5 and 6, and proposes to delete this wording. Also, it is concerned by the large scope of the so-called 'miscellaneous category of data subjects' (Article 5(1)(e)) about whom data can be processed. The Working Party suggests reformulating this category to ensure data about non-suspects can only be processed for a very limited amount of time and under strict conditions. The Directive should make clear that stricter rules on time limits and review have to apply to those groups of data subjects referred to under Article 5(1)(b-e).

With regard to lawfulness of processing (Article 7), it is not clear why the provisions under (b), (c) and (d) are included. They seem to be in contradiction with Article 1(1) which defines the purpose of the Directive. The Working Party considers that there is no room for processing data when it is not in line with the general purpose of the Directive. Thus, the provisions under (b), (c) and (d) either need to be deleted, or Article 1(1) needs to be adapted in order to allow for such processing.

The Working Party believes that specific provisions should be introduced relating to the processing of personal data of children, as provided for by the Regulation. In particular, Member States should be compelled to provide age thresholds under which data should not be processed for the purposes of prevention, investigation, detection or prosecution of criminal offences without due justification, in particular if special categories of data are to be collected. In addition, shorter storage periods in police and justice files should be provided by Member States for data concerning children.

The provision on special categories (Article 8) is slightly wider than in the framework Decision (2008/977/JHA). The Working Party questions the implications of this and especially whether the derogations in paragraph 2 could lead to a general clause in the national law stating that all sensitive data can be processed. In this case, the general prohibition serves no purpose. In addition, despite the inclusion of genetic data, there is no separate recital nor an article on the handling of this kind of data. Such provision would however mean an important safeguard in relation to the use of genetic data and its retention periods.

Based on the derogation in Article 8(2) there is a real danger of allowing different levels of protection of personal data of special categories (sensitive data) under the Directive. The Working Party therefore suggests the European legislator amends this article to provide for harmonised implementation by further defining the required appropriate safeguards. In addition, the Working Party advises to include in paragraph 2 that the exceptions can only be used when in compliance with the conditions set out in Article 4.

Data subject rights

The Working Party notes and welcomes that, based on Articles 11(1) and 13(1), at least in some Member States, more information could be provided to the data subjects. To be informed on what data is being processed and for what reason, is one of the key aspects of the right to data protection. However, it has to be noted too that the limitations to the obligation to inform the data subject and to the right of access as foreseen in Articles 11(5) and 13(2) are problematic. The Working Party regards these limitations and exemptions to be too broad and of a too general nature, since they allow Member States to exempt entire categories of data from the information to be provided. This would severely limit the data subjects' rights (and not only their interests as set out in chapter II). The Directive should therefore make clear that any limitation to the data subjects' rights can only be justified on a case-by-case basis, taking due account of the circumstances of the specific case and that each of these restrictions (and not only omission) has to be fully documented. The Working Party furthermore believes that a limitation to the right of access and information should also mean, that in certain cases, data subjects can still be partially informed of the processing of their data.

With regard to restrictions on rights, there is a need to stipulate that the controller should assess on a case-by-case basis whether the restriction to the rights should apply, and that any restriction must be in compliance with the Charter of Fundamental Rights of the European Union and with the Convention for the Protection of Human Rights and Freedoms, and in line with the case law of the European Court of Justice and the European Court of Human Rights, and in particular respect the essence of these rights and freedoms. The Working Party recommends including this wording in Article 13.

The Directive seems to be consistent with the Regulation relating to the right to rectification, the right to lodge a complaint, the right to a judicial remedy against the national DPA, data controller and data processor, and the right to compensation and liability.

However, the Directive does not provide any right to object to the processing of personal data. There are many situations where, for example, data subjects, victims or witnesses should be able to have their data marked to limit further processing at the end of legal proceedings.

Also, in the Directive data controllers are required to respond to requests from individuals exercising their rights of access, rectification and erasure 'without undue delay'. It is not clear why the same timeframes required under the Regulation cannot also apply here. Moreover, the way the rights of individuals can be exercised needs to be aligned more with the procedures described in the Regulation.

Data controller obligations

The obligations on data controllers are consistent with those under the Regulation as regards processors, arrangements with joint controllers, mandating co-operation with the national DPA, and the tasks of the Data Protection Officer (DPO). However, under the Directive the data controller is not obliged to inform the individual if they intend to transfer personal data to a third country, and it is not clear why this has been excluded, particularly given member states are able to restrict the rights of individuals in certain circumstances.

In addition, the wording of the Directive is not consistent with the Regulation as regards data protection by design and by default and the Working Party sees no reason for this inconsistency. One aspect of privacy by design is determining the risks of processing early on in the process and being able to mitigate those risks. Therefore it urges to insert in the Directive provisions requiring a data protection impact assessment (DPIAs), including during the legislative procedure. It believes these are particularly important in the field of law enforcement processing of personal data, given the increased risks to individuals of this processing. The obligations relating to documentation also contain less detail than in the Regulation. The competent authorities covered by the Directive should at least also need to keep details of their DPO and retention periods.

The Working Party notes that the demands regarding the security of data are not very detailed and thus rather low compared to the current standards. For instance, the security obligation provisions do not include guarding against accidental loss or damage, as is provided for under the Regulation. The Working Party urges the European legislator to include this element in the Directive particularly as this aspect is present in both the current Directive (95/46/EC) and the data protection framework Decision (2008/977/JHA).

Provisions on breach notification should also be consistent across both instruments, however, the Working Party recognises the differences in the law enforcement sector as regards notifying individuals. For example, it may not always be feasible to inform individuals of a breach within specified timescales as this could prejudice law enforcement investigations or operations. The DPA can also have a specific role in assessing the need and appropriate moment to inform the individual, also taking into account the appropriateness of the technological protection measures.
Finally, the provisions on profiling and automated processing (Article 9) are inconsistent with the Regulation in that the Directive wording does not include relevant elements such as evaluating behaviour.

International transfers

General principles for transfers and onward transfers

Article 33 contains provisions both for the original and the onward transfers to third countries or international organisations of personal data. The Working Party considers there is a need to make a clear distinction between those situations, allowing for additional restrictions for onward transfers, for example, taking into account a clear link to the purpose for which the data were originally collected and the prior consent of the sending authority. Furthermore, the recipient of the data needs to be a competent authority in the meaning of the Directive.

Negative adequacy decisions

The Working Party considers it is unclear what the purpose of the non-adequacy decisions is and how these would work in practice. The wording suggests that a non-adequacy decision would block all international transfers to a specific third country, international organisation or processing sector. Articles 34(6) and 35(1) can however also be read in such a way that allows for transfers to declared non-adequate countries, as long as the self-assessment of adequacy carried out by the controller and/or processor leads to a satisfactory result and appropriate safeguards have been agreed upon. The European legislator is therefore requested to adapt the provisions in such a way that it would be clear what the consequences of a so-called non-adequacy decision would be and how they would work in practice.

Transfers by way of appropriate safeguards

The Directive foresees in Article 35 a possibility to transfer personal data to third countries or international organisations in situations where the Commission has not taken a decision on the adequacy. The Working Party considers that if such transfers are made on the basis of a self-assessment, the competent authority needs to ensure the appropriate safeguards are laid down in a legally binding instrument.. Furthermore, the Working Party considers that the elements set out in Article 26(2) of Directive 95/46/EC need to be included, which as a minimum should be taken into account when making the self-assessment. The process leading to the self-assessment needs to be fully documented and be made available to DPAs upon request.

Derogations

The Working Party is concerned about the derogations provided to transfer personal data without an adequacy decision or appropriate safeguards (Article 36) and especially those under (c), (d) and (e). These exceptions would leave room for many international transfers in

individual cases, as long as they are 'necessary'. It must be clear that any derogation must be interpreted restrictively so that transfers done on this basis are the exception rather than the norm. It should also be avoided that the wording of the provisions could mean that a mere statement that the specific transfer is to be deemed necessary without further explanation would suffice to invoke these derogations and thus provide for extensive international transfers on a case-by-case basis without there being any safeguards in place for the protection of the personal data of the individual concerned. The Working Party therefore considers that the wording of Article 36(c), (d) and (e) should narrow down the possibility of international transfers in individual cases.

Furthermore, the Working Party notes that there is no obligation included to ensure that the use of any of the derogations under Article 36 is to be documented. That would make it hard, if not impossible, for the supervisor to verify whether or not the conditions of the derogations have been met by the controller and/or processor. We therefore propose to include such an obligation by adding: "*2. The use of these derogations must be documented and the documentation must be made available to the supervisory authority on request*".

Finally and in general as regards international transfers where no adequacy decision is available, the Working Party considers that Member States should have the possibility to decide whether and to what extent DPAs are involved in international transfers.

Powers of DPAs and co-operation

The Working Party regrets that the provisions related to the powers of DPAs are not very detailed, nor in line with those included in the Regulation. Specifically, the Directive does not include provisions relating to access to premises as is provided for under the Regulation. The ability for the regulator to access the premises of the data controller when necessary should apply to all sectors.

The Directive provides for mutual assistance between DPAs, however, it does not contain the timescales prescribed in the Regulation. This risks a lack of consistency and the advice given relating to the timescales under the Regulation should be taken into account for both instruments. Equally, to ensure consistency across the two instruments, the Directive should include the possibility for DPAs to participate in joint operations.

What is missing

The Working Party regrets that the Directive does not contain provisions on the establishment of time limits, review and other safeguards as the limitation of use of data for serious crimes etc. The Working Party takes note of Article 37 which provides for an obligation by the controller to inform the recipient of any processing restrictions and to take all reasonable steps to ensure they are met. However, Article 37 only applies to transfers to third countries. No justification is provided why the Directive does not include a similar rule when personal data is transferred between Member States of the Union. In such cases, the receiving Member States should also be obliged to respect any limitation of processing imposed by the transferring Member State. The Working Party is surprised that the Directive, in this respect, is a backwards step as compared to the Framework Decision 2008/977/JHA.

The Working Party notes that there is no obligation for the competent authorities that have transmitted data to inform the recipient that the transmitted data were incorrect or unlawfully transmitted. Such an obligation is crucial in an area of free flow of law enforcement information. Article 39(2) contains the possibility for Member States to decide that the DPA responsible for supervising the Regulation and the Directive may be the same. Taking due account of the national situations, especially in countries with sub-national DPAs, the Working Party would prefer if indeed a single DPA would be responsible for supervising both instruments. This would ensure consistency in the application of the rules.

The Working Party finally regrets that the Directive does not contain a provision on the transfer to private parties or other authorities, which are not a competent authority under the Directive. The Working Party therefore urges the European legislator to introduce a provision, allowing for transfers of law enforcement data to private parties only in narrowly defined circumstances defined by law.

Done at Brussels, on 23rd March 2012

For the Working Party
The Chairman
Jacob KOHNSTAMM

The Belgian Data Protection Authority and the Romanian Data Protection Authority choose to abstain from voting for the only reason that they do not support the choice for a Regulation as the appropriate legal instrument.

The Data Protection Authority of the Czech Republic also abstained from voting.

The Estonian Data Protection Authority voted against the opinion, because they doubt whether the proposed reform packet is in line with the declared purposes. The Estonian Data Protection Authority sees too many essential disconcerting aspects in the packet such as:

1) missing of proper impact assessment (negative opinion by impact assessment board),
2) form of directly applicable regulation for a framework legislation,
3) higher administrative burdens,
4) extent of delegated legislation,
5) weakening of national DPAs, protection of time-critical privacy rights is going farther away, prolongation of protection measures,
6) competence issue with draft data protection directive on police and criminal justice,
7) contradiction of the principle of subsidiarity.

Therefore the Estonian Data Protection Authority can not agree with the main conclusions:

1) the draft regulation is too weak to have “general positive stance”,
2) we do not think that the draft data protection directive in police and justice area is too modest. We think that this is too far going because of lack of legislative competence in domestic procedural law.