17 June 2015

Appendix

Core topics in the view of trilogue

Following the opinions and statements already issued relating to the data protection reform[1], the Working Party would like to express its views on some identified areas of concern that need further attention in the perspective of the trilogue between European institutions.

It is crucial that the results of these negotiations lead to the adoption of new regulatory framework respectful of the fundamental rights of the individuals and that takes into account the interests of all stakeholders. The Regulation should also be as simple, efficient and clear as possible. It must be appropriately balanced in order to guarantee a high level of protection of the individuals and allow companies to preserve innovation and competitiveness. Furthermore the text of the Regulation should refrain from going into matters of detailed implementation. These should be left to guidance and rules of procedure to be developed by the EDPB. The Working Party would appreciate the possibility to start working on guidance and rules of procedure from the date of adoption of the regulation.

Chapter I/ General provisions

1/Subject matter and objective

The Council of the EU provides Member States with the possibility to introduce "more specific provisions to adapt the application of the Regulation with regard to the processing of personal data for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for other specific processing situations".

The Working Party underlines that if this provision is maintained, it should be understood as a possibility given to Member States to specify and adapt the rules of the Regulation without lowering its level of protection.

[1]WP191, WP199, WP222 Additional statements on the reform package of 27.02.2013, 11.12 2013 and 16.04.2014

While recognizing the need for local customization in certain cases, the Working Party would like to strongly underline that such given flexibility should not undermine the level of protection brought by the Regulation and that harmonization of a high level of protection remains the goal.

Material scope

Frontiers between the Regulation and the Directive

Situations must be avoided where the same data processing (i.e.: processing for administrative purposes) is subject to differing rules (i.e.: Regulation or Directive) which do not potentially provide the same level of guarantees.

Indeed, even if the Directive should be regarded as minimum standard allowing the Member States to provide additional safeguards, an extension of its scope as proposed by the Council of the EU to all processing activities for the "safeguarding against and the prevention of threats to public security" - in addition to processing activities carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties- would result in a different level of protection depending on its implementation.

Moreover, the notion of "the prevention of threats to public security*"* not linked to the concept of criminal offences is quite vague and may open the door to including in it types of processing operations just because they are carried out by controllers that operate in the widest context of law enforcement.

Additionally such extension would include an indefinite number of authorities whose tasks may be only occasionally linked to that purpose into the scope of the directive.

It would lower the level of data protection in the public sector from the one proposed by the Regulation. There is no compelling reason to create such flexibility and to exclude the activity of public security from the Regulation.

In order to ensure a consistent and high level of protection, the Working Party is of the opinion that the processing activities performed for purposes not linked to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be clearly maintained under the scope of the Regulation.

In addition, it must be ensured that the 'core' aspects of both texts are consistent and uniformly understood, irrespective of the legal instrument chosen in order to avoid confusion and overlap impacting the level of protection guaranteed to individuals.

This is particularly true for the definitions, principles, obligations, individual's rights and powers of supervisory authority.

The household exemption

The Council of the European Union has broadened the so-called household exemption in Art. 2(2)(d) of the Regulation by deleting the words "without any gainful interest" and "exclusively" which has been included in the EU Commission's version and by referring to recital 15 providing that household activity implies no connection with a professional or commercial activity.

The Working Party recognizes the Council of the EU's aim to slightly broaden the scope of the household exemption in order to limit the scope of the Regulation but feels that any exceptions to the rules shall be formulated and interpreted restrictively.

Moreover, further details to define "purely" household activities may be elaborated by DPAs and/or EDPB.

The Working Party is in favour of a limited and carefully balanced household exemption applying to "purely" household activities as provided for in Directive 95/46/EC and interpreted by ECJ case law.

The territorial scope

The EP foresees that the Regulation applies only to non-EU processors in addition, to non–EU controllers where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the European Union

Considering the introduction of another legal liability for processors separate from the controllers' in the Regulation, it would be advisable to subject to the Regulation the processing activities from processors non-established in the EU where they are processing of personal data on behalf of data controllers subject to the Regulation. Otherwise, the legal regime will be different whether the processor is outside or inside EU. For those established in the EU, the liability will be framed by the Regulation and directly enforceable by the data subject. On the contrary, for non-EU processors, the liability will remain a contractual liability as it is today.

The Working Party would like to draw attention to the need to cover non-EU processors where they act for controllers subject to the Regulation.

Definitions

Consent

There should be no doubt on the elements establishing consent and the intention of the data subject to consent.

Even though it can be expressed in many different ways, for instance through a statement or an affirmative action, the essential requirement is that such statement or action must clearly signify the data subject's agreement to personal data relating to them being processed. There has to be a clear distinction between opt-in and opt-out.

Therefore, the notion of unambiguous consent foreseen by the Council of the EU in Recital 25 may create some confusion with respect to the aim of the proposed text especially on the Internet where there is now too much improper use of consent.

Requiring it to be *explicit* is an important clarification, truly enabling data subjects the exercise of their rights.

Furthermore consent should be informed and concern a specific purpose, any ´broad consent´ would therefore not be acceptable.

The Working Party expresses its support for proposals requiring that the consent should be informed, given for a specific purpose, freely and explicitly.

Personal data

A natural person can be considered identifiable when, within a group of persons, they can be distinguished from others and consequently be treated differently. This means that the notion of identifiability should include singling out individuals.

The Working Party expresses its support for a recital clarifying that the capacity to single out and treat differently is a means to identify the data subject.

However, the Working party considers that Recital 24, as proposed by the European Parliament and by the Council of the EU, is not satisfactory as it could be interpreted in a way that identification numbers, location data, online identifiers or other specific factors will not be necessarily considered as personal data. This could lead to an unduly restrictive interpretation of the notion of personal data.

The Working Party reiterates that IP addresses, online identifiers, or other specific factors should be considered, as a general rule, as personal data, as also stated in several CJUE rulings[2].

Pseudonymisation

Pseudonymising techniques used to disguise identities and enable the collection of data relating to the same individual without having to know their identity can help reduce risks to individuals.

Regulation should treat the process of pseudonymisation as a system of data minimisation. A new category of "pseudonymised" or pseudonymous data may lead to confusion and constitute a Trojan horse for unjustified specific derogations (e.g. as a presumption of legitimate interest of the data subject).

For instance, it should only be considered as a method applicable to controllers who already process usual identifiers (such as name, address) but then decide to separate the information

[2] CJUE 29 January 2008 Promusicae (C-275/06), CJUE 8 April 2014 Digital Rights Ireland ltd (C-293/12)

and create aliases. As a privacy tool, it helps to minimize the processed information and, subsequently, the risks (e.g. in the scientific sector where 'key coded data' is processed).

The Working Party expresses its support for referring to the pseudonymisation as a security measure and is opposed to introducing a new category of data with the notion of "pseudonymous data".

Chapter II/ Principles

Purpose limitation

The purpose limitation principle is one of the key data protection principles. It is designed to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use. The controller must only collect data for specified, explicit and legitimate purposes, and once data are collected, they must not be further processed in a way incompatible with those purposes.

Purpose limitation protects data subjects by setting limits on how controllers are able to use their data while also offering some flexibility for controllers.

The Working Party is of the opinion that permitting controllers to further process data for incompatible purposes as long as they find a new suitable legal basis erodes this cornerstone principle.

In particular, the Working Party considers that by enabling a controller to process data in an incompatible way when the controller has an overriding interest in the processing, further processing will be trivialized to such an extent that it will pave the way to putting into question the fundamental principle of purpose limitation.

According to the present legal framework, processing of personal data in a way incompatible with the purposes specified at collection is against the law and therefore prohibited. The controller cannot legitimize incompatible processing by simply relying on a new legal ground. The new legal provisions should ensure at least the same level of protection offered by the current Directive.

Further processing should only be permitted once compatibility is established after a careful assessment that takes into consideration all relevant circumstances of both the original and the subsequent processing operations and provided that the controller may find an adequate legal basis. Compatibility should not be confused with legitimacy.

Establishing that further use is compatible with the initial one does not mean that data may be processed without a valid legal basis or relying in the legal ground that legitimized the original processing. Compatibility and legitimacy are cumulative requirements and, for a change of purpose which is not incompatible, one of the legal bases has to be applied.

The Working Party strongly recommends the deletion of paragraph 6.4 of the proposal that provides for the possibility for a controller to further process data if the purpose is incompatible with the original one.

Processing for compatible purposes should always need its own legal basis.

Processing necessary for the purposes of archiving, historical, statistical and scientific research

The paragraph 6.2 is drafted in a way that might be interpreted as setting a new and independent legal basis by virtue of which processing for historical, statistical, scientific research (and archiving in the Council of the EU version) would be legitimate without the need to rely on other legal basis and provided that conditions and safeguards of Article 83 are respected. It should be made clear that the second paragraph of Article 6 does not exempt the need to also comply with the first paragraph of Article 6. Any kind of processing should comply with the lawfulness test.

Moreover Article 9(2)i. of the latest Council of the EU's draft would appear to also legitimate the processing of sensitive data for these purposes per se, without the need for a specific legal basis.

In addition, Article 83 of the Council of the EU enables Member States to introduce many derogations on the rights of the data subjects.

On the other hand, the common position adopted by the European Parliament seems to set unnecessarily restrictive conditions for the use of personal data concerning health in the context of historical, statistical or scientific research purposes, which will only be possible with the consent of the data subjects. Although the same article allows Member States to provide for exceptions with regard to research that serves a high public interest, this limitation in the choice of legal basis for the processing of health data for statistical, historical or scientific research purposes seems to go beyond what is necessary in order to protect the rights of data subject and may hamper processing operations which might be legitimate on the basis of other legal grounds**.**

Further processing for the purposes of archiving, historical, statistical and scientific research should be presumed as compatible with the initial purpose of collection. They must be

grounded on a legal basis under Article 6.1 and meet the requirements of Article 9.2. Any impact on the applicable rights and obligations should also be framed in the Regulation. The position of the Council of the EU to only rely on national law will prevent harmonisation in this field while historical, statistical and scientific research needs to be more and more EU transnational (i.e., EU funding promotes cross EU national activities).

In addition, the Working Party would really like to caution for the deletion of the word "research" by the Council of the EU (also in Article 6). This could potentially open up a pandora's box for apparently historical and/or statistical purposes by the private sector other than for research.

The Working party strongly supports the following elements

- Further processing for scientific, historical, statistical and archival purposes should be considered as compatible with the original purpose of collection;

- Processing (be it original or subsequent) for scientific, historical, statistical research and archival purposes should always be based on one of the legal basis of Article 6.1 and meet the requirements of Article 9.2 if needed.

Legitimate interest using pseudonymous data

The use of pseudonymous data as a means to provide safeguards to ensure fair processing of personal data may play a role in determining whether the legal ground of legitimate interest can be legally used.

This, however, remains only one factor amongst many and the balancing test always requires to also assessing the purpose of the processing.

The Working Party does not support provisions which could be interpreted as an exemption for the controller's obligation to carry out the important balancing test when processing pseudonymous data.

Processing not allowing identification

The Working Party is concerned about a broad interpretation which could be given to Article 10 as proposed by European Parliament.

Article 10 as proposed by European Parliament can lead to exempt controllers or processors from complying with the Regulation when processing pseudonymous data.

Pseudonymous data, given that they permit to single out and treat differently a natural person, remains personal data and their use should not exempt controllers/processors from complying with obligations provided by the Regulation (e.g. key principles, accountability obligations…).

However, a controller should not be in a position to be obliged to collect more information from the data subject for the purpose of exercising their rights if it cannot directly identify the data subject. From the moment the data subject could be authenticated, the exercise of their rights should be made possible. In practice, if a controller is singling out data subjects on the basis of digital identifiers, data subjects should be entitled to exercise their rights by authenticating himself/herself with those digital identifiers.

The Working Party supports propositions clarifying that if the purposes for which the controller processes personal data do not or no longer require direct identification of the data subject by the controller, the controller shall not be obliged to maintain or acquire additional information nor to engage in additional processing for the sole purpose of complying with articles 15, 16, 17, 18 except where the data subject requests so and provides additional information enabling his or her authentication.

Chapter III/ Rights of the data subject

Information to the data subject

The Working Party finds that the informational elements on security measures, retention period, applicable safeguards in regard to third country transfers, and on the underlying logic in data processing should be communicated to the data subjects.

Information to the data subjects can be provided by using layered privacy notices disseminating the requested information in an easily readable format.

The Working Party supports proposals specifying that information relating to further processing, the data retention period, the safeguards put in place for international transfers, security measures should be provided by the controller to the data subjects.

RBA in the rights of the data subject

As stated in its previous opinion[3], the Working Party underlines that the rights granted to data subjects by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved (e.g. right of access, rectification, erasure and objection, transparency, right to be forgotten, right to data portability).

Therefore, some references in the Council of the EU position to the necessity of "taking into account the circumstances" or "having regard to the purposes" when granting rights to the data subjects, are creating uncertainty and potentially room for interpretation that could lead to lowering the level of protection for data subjects.[4]

Data Portability

One of the aims of the right to data portability is to empower the individual to control his/her personal data.

In order to ensure greater effectiveness of this right, data subjects should be able to transmit personal data related to him/her or to a third person from the moment it has been provided by him/her.

[3] WP218 Statement on the role of a risk-based approach in data protection legal. 30 May 2014

[4] See for example article 16 of the Council position: "Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data (…).

In addition, the data shall be, at the request of the data subject, transmitted directly from controller to another one.

This should apply to all types of processing whatever the legal basis being used for that processing.

The Working Party supports proposals with respect to the broad scope and content of the right to data portability but is in favour of maintaining this right under Article 18 as a separate and independent new right from the right to access.

Right of access

The right of access for the data subject is a fundamental right that applies even where the personal data of the data subject is also the personal data of one or more other data subjects. In such cases the data controller has to balance the right of access for the requesting data subject with any prejudice to the rights and freedoms of other data subjects that granting such access might cause.

This is provided for by restrictions on the rights of data subjects where they are a necessary and proportionate measure to protect the rights and freedoms of others.

Any blanket restriction of access to personal data that is also the personal data of other data subject would be a reduction in the rights of data subjects currently provided for under Directive 95/46/EC.

Therefore, the Council of the European Union's proposal limiting the right to obtain a copy of it personal data when disclosing personal data of other data subjects could lead to reduce the right of access.

The Working Party considers that a blanket restriction of the right of access for the data subject to personal data that is also the personal data of other data subjects is unjustified on privacy grounds and would be a reduction in the existing rights of data subjects.

Right to object

The Working Party is concerned by the proposal of the Council of the EU which proposes to limit the exercising of the right to object to the sole case where the data processing is founded

upon the legitimate interest of the controller or upon the public interest or in the exercise of official authority vested in the controller [5].

This proposition will pave the way to an unacceptable decrease in the current level of protection established by the Directive 95/46/EC and by its transposed laws within Member States.

Taking account of what is feasible, the Working Party supports extending the right of the data subject to object beyond that currently established by Article 14 of Directive.

Restrictions

New grounds have been added by the Council of the EU to allow derogations from data subjects' rights (Articles 12 to 20 and 5) such as "important objectives of general public interests of the Union or of a Member State, and the enforcement of civil claims".

The Working Party notes that such very general and vague derogations go further than the legal grounds currently permitted under the Directive are contrary to legal certainty and constitute a breach in the "community acquis".

In addition, the Working Party is of the opinion that the legislative measure restricting the rights and obligations to be adopted according to Article 21 § 1, should always meet the requirements of Article 8 § 2 of the European Convention on Human Rights and the relevant case-law of the European Court of Human Rights and of Article 8 of the Charter of Fundamental Rights of the European Union.

Accordingly, these legislative measures shall contain, as a matter of principle and not only "where relevant" (as proposed by the Council of the EU) the purposes of processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the specifications of the controller or categories of controllers and the applicable safeguards taking into account the nature, scope and purposes of the processing and risks for the rights and freedoms of the data subjects.

[5] EU Council/ Article 19.1 "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on points (…) (e) or (f) of Article 6(1), the first sentence of Article 6(4) in conjunction with point (e) of Article 6(1) or the second sentence of Article 6(4).

Profiling

Profiling has found its way into many areas of life (e.g.: consumer profiles, movement profiles, user profiles and social profiles). Due to the widespread availability and possibility of linking data on the Internet, data subjects can be subject to insufficient transparency and therefore may feel unable to exercise sufficient control over the processing of their personal data.

In its previous Opinion[6], the Working Party underlined the necessity to provide more legal certainty and more protection for individuals with respect to data processing in the context of profiling. It identified the need to introduce a clear definition of profiling following the Council of Europe's approach.[7]

The Working Party estimates that the proposals of the Council of the EU [8] are unclear and do not foresee sufficient safeguards which should be put in place.

The Working Party renews its call for provisions giving the data subject a maximum of control and autonomy when processing personal data for profiling.

The provisions should clearly define 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.

The Working Party suggests modifying the Article 20 by adding provisions relating to the purposes for which profiles may be created and used and specific obligations on controllers to inform the data subject.

[6] Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation/13 may 2013

[7] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling

[8] Article 20.1b Obligation for controller to "*implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, such as the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*

Chapter IV/ Obligations on data controllers and processors

The risk based approach/Accountability

The Working Party considers that accountability is an underlying principle of privacy and data protection that should not be undermined of its substance by an inappropriate application of the risk based approach.

Controllers and processors should be accountable as a principle for complying with data protection obligations including demonstrating compliance regarding any data processing whatever the nature, scope, context, processing purposes or possible risks for data subjects.

The Working Party is in favour of a recital clarifying that accountability is a fundamental principle which applies to all processing operations.

Representatives of controllers not established in the Union

Exempting controllers not established within the Union from appointing a representative when processing is "occasional and unlikely to result in a risk for the rights and freedoms of data subjects" as it is proposed by the Council of the EU is too vague[9] and could limit the effectiveness of the Regulation. Any exception should be based on objective criteria such as the nature, regularity and scale of the data processing activity targeting the EU that helps to measure the risks. In addition, representatives should have a legal personality in order to make the liability scheme operational and efficient.

Documentation

Documentation is an important tool for controllers in properly managing their data protection responsibilities. Controllers cannot ensure compliance without knowing what personal data they process and how they process them.

Furthermore the keeping of appropriate documentation is a necessary element of accountability, helps to enable the exercise of rights by data subjects and supports ex-post investigations by DPAs. Whilst the requirement for a controller or processor to maintain documentation must be scalable and proportionate to the data protection risks represented by

[9] Art 25

the processing and the nature of the personal data held it should not be subject to any absolute exemptions.

The Working Party considers that, as a general principle, controllers and processors should document their processing activities proportionately to ensure accountability and transparency.

Notification of personal data breaches

The Working party had already pointed out in its Opinion 1/2009, that the rationales for the two types of notification are different and the cases in which DPAs and data subjects have to be informed should also be different. It is essential to provide safeguards ensuring that data breaches are not concealed, that the assessment of the breach is correctly carried out and that data subjects are notified whenever it is required. Authorities should be notified in a larger number of cases than data subjects, so they can be in a position to exercise supervision over the process of notification to data subjects by service providers. In this respect the notion of high risk for the rights, freedoms and interests of data subjects necessarily cannot be the only factor that triggers notification to DPAs.

In addition, the Council of the EU proposal foresees that controller who has taken subsequent measures to ensure that high risks for the data subject are no longer likely to materialize is exempted from notifying the data subject and the DPA.

Such derogation is too broad and may have the effect of giving most controllers a ground not to inform the relevant stakeholders.

In addition, notification to data subjects should not be mandatory when it "is likely to result in a high risk…" but rather when, to a significant extent, "the personal data breach is likely to adversely affect the personal data or privacy" of the data subject. This would allow to align the criteria with the ePrivacy directive and to build on the guidelines already published by the Working Party and the ENISA.

The Working party supports different thresholds for notification of personal data breaches to the authority and the individuals.

As regard notification to the data subjects, the Working party also supports an alignment with the wording already used in the ePrivacy directive (notification to the data subjects when the "personal data breach is likely to adversely affect the personal data or privacy of a data subject…")

Data Protection Impact Assessment (DPIA)

According to the text of the European Parliament, the DPIA becomes a second step after a preliminary risk analysis to be conducted by all controllers (and, where appropriate, processors). A DPIA would be required where a specific risk is identified i.e. in case the processing belongs to a list of 'risky' operations set out in Art. 32a) and would have to be periodically reviewed. Although this two-step approach assessment seems very complete, it will probably require lot of work, resources and investment from companies, especially SMEs.

The Working Party welcomes the approach to DPIA which takes into consideration the wider perspective of impact on the rights and freedoms of the data subjects, rather than focusing exclusively on the protection of personal data. Assessing the impact that an unlawful processing of personal data may have on the wider portfolio of rights and freedoms should also underpin the proposed methodology. The reference to the entire lifecycle of personal data processing as a context of the assessment and a short description of essential content elements would be particularly valuable.

In addition, the Working Party does not see reason why excluding public authorities from doing PIA unless the processing result from a legal obligation (EU or Member states law) and the DPA has already been consulted.

The Working Party expresses its support for DPIA approach which takes into consideration the wider impact on the rights and freedoms of the data subjects, rather than exclusively the impact on the protection of personal data. The reference to the entire lifecycle of personal data processing would be particularly welcome.

DPA Consultation

The Working Party recalls that the controller and the processor are themselves responsible to ensure compliance with the Regulation. The approach to mandatory consultation of the DPA should be compatible and consistent with the principle of accountability.

The Working Party considers that prior consultation of DPAs should be limited to situations where their intervention is particularly necessary to safeguard the rights and freedoms of the data subjects.

The Working Party considers that an approach to mandatory consultation of the DPA should be consistent with the principle of accountability.

Data Protection Officer

The DPO is a cornerstone of accountability and a real tool of competitiveness for companies. Tasked with the implementation of accountability tools (e.g.: documentation, PIA, etc…), they should be considered as the "compliance orchestrator" and the intermediary between all relevant stakeholders (e.g. supervisory authorities, data subjects, business partners).

The Working Party considers that the reference to national law, as proposed by the Council of the EU[10], will increase the risk of fragmentation between Member States and undermine the DPO's usefulness.

The Working Party supports the appointment of DPOs as a mandatory obligation subject to objective criteria such as the type, volume of data or nature of activity of the concerned entity that helps to measure the risks.

[10] Article 35 : The controller and or the processor may, or where required by Union or Member State law shall designate a data protection officer

Chapter V - Transfers

Adequacy principle

The adequacy principle which is one of the key principles of the current EU regulatory framework (Article 25 of the EU Directive) should be reflected and expressly stated into the Regulation. Even if the adequacy principle is integrated into the Regulation's sections dedicated to Commission's adequacy decisions and to other transfer tools, the Article 29 Working Party insists on the need to reaffirm the general adequacy principle as the corner stone of the EU regulatory framework.

The Working Party is in favour of ensuring the Regulation includes the principle of adequacy as currently covered in Article 25 of the Directive 95/46.

Derogation on the basis of the legitimate interest

The Working Party has repeatedly expressed its concerns about adding such broad derogation under Article 44 h) allowing transfers to non-EU countries for the legitimate interest of the controller based on assessment of suitable safeguards. The Article 29 Working Party notes that these concerns have been addressed by the proposal of the European Parliament deleting this provision. If this provision is to be maintained, it should at least be on an exceptional basis and only for non-massive, non-repetitive and non-structural transfers.

The Working Party supports that if Article 44 h) is to be retained, it should be only used on an exceptional basis and only for non massive, non repetitive and non structural transfers, subject to guarantees, and in particular, to specific information obligations vis-à-vis the data subjects.

Processors and subprocessors

The Regulation provides for an enlarged role for processors by ensuring adequate data protection with respect to the framework of their own transfer's data and also by considering the introduction of the accountability principle.

BCRs for processors are based on the accountability principle and are a valuable tool to demonstrate compliance with data protection obligations. They are also a useful means to ensure, as much as possible, a good level of protection when transferring data.

In addition, the Working party welcomes the proposals of the Council of the EU made under paragraphs 1A and 2A of Article 26 to incorporate the rules relating to sub-processing activities (already developed in the BCR for Processor) within the EU.

The possibility for processors to sub-contract part of their activities is more and more used in practice, in particular in the context of the development of the cloud computing, and it is important for the regulation to address such development.

The Council of EU' position aims to avoid any confusion of roles between processors and controllers[11], to bring legal certainty[12] but also leave some flexibility for the contracting parties[13]. The conditions proposed under those paragraphs clearly reflect the position already taken by the Working Party and are therefore welcome[14].

The Working Party is concerned about the deletion of the possibility of BCR for Processor (BCR-P) and considers it essential to re-insert them.

However, the Working Party supports proposals that set clear legal conditions for the possibility for processors to sub-contract part of their activities, and in particular in the context of the development of the cloud computing. Legal conditions should ensure that the controllers remain into control, have full transparency on sub-processing activities and that the level of protection is maintained during the entire cycle of processing.

Access by public authorities

The Working Party welcomes the introduction in the Regulation of the principle according to which disclosure of personal data to any authority of a third country (court, tribunal, administrative authority) should only take place after the notification of the request and prior authorization of the competent supervisory authority, without prejudice to a Mutual Legal Assistance Treaty or an international agreement in force between the requesting third country and the Union or a Member State. It is also welcome that the authorization given by the supervisory authority should be based on an assessment of the compliance of the request with

[11] By imposing the need of transparency towards the controller and its prior authorization which enable the later to remain into control.
[12] By imposing that the sub-processor will be contractually bound by the same duties than the main processor and ensuring that the main processor will be responsible for any breach caused by its sub-processor.
[13] By giving the choice to the controller for a specific or general authorization combined with an opt out mechanism.
[14] WP196 on cloud computing and WP195 on BCR Processor.

the General Data Protection Regulation, and the competent national law enforcement authority should be informed of said request.

The Working Party considers that the scope of the provision should be broader than judgments of foreign courts or tribunals, or decisions of administrative authorities, and should encompass any access on behalf of public authorities or governmental bodies of third countries.

In this respect, for law enforcement authority requests, a more transparent legal framework such as the use of Mutual Legal Assistance Treaties (MLATs) or existing international agreements in case of disclosures not authorised by Union or Member States' law, should remain the principle. The Working Party does furthermore believe that in cases where a MLAT (or comparable international agreement) is in place, the competent authority under the MLAT (or comparable international agreement) should be the authority dealing with the request rather than the data protection authority. Naturally, where necessary, the competent authority under the MLAT should consult the data protection authority where appropriate.

In cases where cooperation channels do not exist and where it is difficult to identify the so-called "competent authority" or where there isn't any, the controller or processor should notify the competent DPA.

The Working Party considers the question of disclosure of personal data to authority of a third country (court, tribunal, administrative authority) is a very important issue and welcomes the principle of notification of such request to DPAs.

The Working Party is also of the opinion that in cases where a MLAT (or comparable international agreement) is in place, the competent authority under the MLAT (or comparable international agreement) should be the authority dealing with the request rather than the data protection authority in cases where cooperation channels do not exist and where it is difficult to identify the so-called "competent authority" or where there isn't any such authority, DPAs should be competent and duly informed.

Chapters VI, VII, VII Governance

One-Stop-Shop mechanism

The Working Party welcomes the improvements made by both institutions on this core topic and which reflect the concerns previously expressed in Article 29 Working Party documents[15]. More precisely, both institutions foresee that:

- All supervisory authorities remain competent on their Member State territory,
- Cooperation shall take place between all concerned DPAs and a designated lead DPA on cross-border cases.
- EDPB issues binding decisions where necessary.

In addition, to ensure proximity with citizens, the Council of the EU has added valuable elements:

- DPA are competent where individuals on their territory are affected by data processing by controllers and processors established within or outside the EU.
- The cases of pure national or minor cross-border relevance are left to the DPA.
- Citizens have the possibility to seek remedies in courts within their own Member State.

The Working Party would like to express its support for a solution which ensures proximity with citizens and a uniform response to companies.

The Working Party recalls that the cooperation process should be simple, clear and efficient for all stakeholders in order to ensure an effective supervision in all circumstances. Implementation details should be left to the EDPB to develop rather than being spelled out in the Regulation.

[15] WP29 Statement - main points for one-stop-shop and consistency mechanism for businesses and individuals - April 16, 2014.

Powers of DPAs/Sanctions

In order to be effective, the Regulation should provide efficient tools for data protection authorities. The power to suspend data processing, to bring processing operations into compliance in a specific manner and impose fines that are sufficiently dissuasive, severe and proportionate is crucial to ensure compliance. The Working Party recalls that the whole range of DPAs powers, including fines should apply wherever the controller is a public or a private entity.

The Working Party welcomes the introduction of significant fines to enable DPAs to take up their role as enforcement authorities and can contribute to a higher degree of compliance by data controllers both in the public and private sector. In addition, the DPAs must have the right to prioritize their workflows and to focus on matters which substantially impact the rights and freedoms of data subjects.

The Council of the EU does not foresee an administrative fine in case a controller or processor does not comply with its obligations under Art. 53(1)[16]investigative powers of the DPA. For the day-by-day business of data protection supervision, in particular carrying out inspections, the investigative powers of the DPA are key elements of effective data protection supervision. In reality DPAs may be confronted with the situation that controllers/processors do not comply with their obligation to endure those investigations. This especially applies where a controller or processor refuses to answer the DPAs requests.

The Working Party deems it necessary to introduce an administrative fine in cases where a controller or processor does not comply with its obligations under Art. 53(1)

Representation of data subjects/ Right to lodge a complaint

The Working Party welcomes the Article 76 as it aims to facilitate the access of data subjects to judicial remedy.

The Council of the EU foresees the possibility for any body, organisation or association, to lodge a complaint with the supervisory authority independently of a data subject's mandate or complaint (Art. 76.2).

[16] According to the Commission's as well as the Parliament's proposal the obligations to cooperate are provided for in Art. 29 which has been deleted by the Council

This possibility should however be respectful of the interest of the data subjects and not lead to abuse of data subject's rights, or to exercise any pressure or influence on the supervisory authorities.

The Working Party considers that the possibility to public or private organisations to submit a complaint to the supervisory authority without any mandate from the data subject should be respectful of the interest of any affected data subjects.