ARTICLE 29 DATA PROTECTION WORKING PARTY

01574/12/EN

WP199

Opinion 08/2012 providing further input on the data protection reform discussions

Adopted on 05 October 2012

Introduction

Since the adoption of the data protection reform package on 25 January 2012, both the Council and the European Parliament have started their respective procedures in the legislative process.

European Parliament

The European Parliament has appointed the LIBE committee as the main committee responsible for both proposals and has appointed Jan Albrecht and Dimitrios Droutsas as rapporteurs. Parliamentary committees that are also involved are IMCO, ITRE, ECON, JURI and EMPL.

The reform package has already been discussed several times in LIBE and with the shadow rapporteurs (members of other political groups dealing with the reform). The rapporteurs have also organised a stakeholders meeting on the draft Regulation on 29 May 2012. On 9 and 10 October 2012 the LIBE committee is organising an Interparliamentary meeting with members of national parliaments to discuss the reform package. The LIBE committee intends to present draft reports on the reform before the end of 2012. The other involved committees would in that case need to present their draft opinions before the end of the year as well.

At a LIBE meeting in June 2012 the rapporteurs presented a first Working Document which highlights the main elements of the reform, calls for a package approach ("*to develop two fully coherent, harmonious and high standard legal instruments as regards data protection by adopting a comprehensive, balanced, coordinated and parallel procedure for both texts*") and identifies several areas in need of further debate and clarification:

1. the role of the Commission through delegated and implementing acts and in the consistency mechanism;
2. the current exclusion of data protection rules for EU institutions and agencies from the reform;
3. the relation between general Union law and national specific laws;
4. the exact division of roles and responsibilities among data protection authorities in crossborder cases;
5. clarifications on profiling, including a human element and a right to information about the logic involved in data processing, as demanded by Parliament;
6. the notions of "legitimate interest", "public interest" and "public security";
7. the inter-linkage of both legislative instruments, especially in cases of law enforcement access to personal data held by private entities;
8. access requests or access orders for personal data stored in the Union by public authorities in third countries, especially for cases where the data controller also has an establishment there;
9. stronger incentives for data protection by design and by default.

Council

Several Council working party meetings (DAPIX) have been held, first under the Danish Presidency and currently under Cypriot Presidency of the Council. The discussions in DAPIX have mainly concentrated on the draft Regulation and have taken an article by article approach.

According to the Council, the discussions at working party level have shown a broad consensus among Member States on the need to reform the existing legal framework on data protection and to strengthen the rights of individuals to the protection of their personal data. Furthermore, a convergence of opinion among Member States has emerged on the necessity to ensure more harmonisation and consistency in the application of EU rules on data protection. However, from a leaked document it shows that several longstanding and key notions in data protection are called in question by several national delegations.

At an informal meeting of the Justice and Home Affairs Ministers in Nicosia on 23-24 July 2012 the Ministers discussed whether certain formal requirements (administrative burden) should not be better tailored – particularly for MSME's– on the basis of agreed criteria, such as the risks connected to the data processing activity, the size of the controller, the amount of personal data processed and/or the number of individuals (data subjects) affected. The Minsters furthermore agreed that there should be no differentiation as such in the rules concerning the private and public sectors although some degree of flexibility for the public sector is necessary. The Minsters also agreed to examine on a case by case basis the need for, timeframe of and possible alternatives to the large number of proposed delegated and implementing acts. To this end, Member States have received a questionnaire (to be answered before 4 October) regarding administrative burden, delegated and implementing acts and the degree of flexibility in data protection rules deemed necessary for the public sector.

Further input by Article 29 Working Party

In its opinion of 23 March 2012, the Article 29 Working Party provided its first general reaction to the Commission proposals, highlighting areas of concern and making certain suggestions for improvement.

The Article 29 Working Party welcomes the so-called "package" approach taken by European Parliament rapporteurs and is confident that all parliamentary committees involved will take careful consideration of all elements of the package in order to further improve both Commission proposals.

The Working Party also welcomes the steps undertaken by the Cypriot Presidency of the Council mentioned above that are meant to reinvigorate discussions in the Council Working Group dealing with the reform.

With a view to the on-going discussions in both the European Parliament and the Council, the Working Party has decided to adopt this opinion providing further guidance, notably on certain key data protection concepts and by analysing the need for and the effect of the proposed delegated acts and where necessary suggesting more suitable alternatives.[1]

The Working Party notes that some of those who have raised concerns about the impact of the proposed Regulation are focussing their attention on the key concepts of personal data and consent. The Working Party believes that this is mistaken. In order to properly protect the privacy of personal information and future-proof the Regulation, it is necessary to adopt a broad definition of personal data and to ensure that where consent is relied on, the consent is of a high standard. If the adoption of these key concepts leads to disproportionate outcomes in the application of the provisions of the Regulation in governing processing and establishing individual rights, it is on those provisions and the exceptions to them rather than on the key concepts themselves that attention should be focussed.

[1] Furthermore, the Working Party is in the process of examining the notion of purpose limitation and intends to adopt an opinion on this issue early next year. The Working Party will also contribute to ongoing discussions on the scope of the Regulation, notably concerning the exemption for household and personal use.

On the definition of personal data

In its opinion of 23 March[2], 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...*".

The Working Party notes that this definition does not fundamentally change the notion of personal data as defined in Directive 95/46/EC, but only reorganises its different elements[3]. In its opinion on the concept of personal data[4], the Working Party has already observed that the present definition offers sufficient continuity and flexibility in the way it applies to data in various contexts, such as pharmaceutical research or IP addresses.

One of the main conclusions of this analysis is that a natural person can be considered identifiable when, within a group of persons, he or she can be distinguished from other members of the group and consequently be treated differently.

It is therefore suggested to clarify in Recital 23 and Article 4 that the notion of identifiability also includes singling out in this way.

Recital 23*: 'The principles of protection should apply to any information concerning an identified or identifiable person* ***and any information allowing a natural person to be singled out and treated differently****. To determine whether a person is identifiable, account should be taken of all the means* ***reasonably*** *likely [delete: reasonably] to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.'*[5]

Article 4 (2): *'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly****, or singled out and treated differently****, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person'.*

Furthermore, 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

[2] Opinion 1/2012 on the data protection reform proposals (WP 191)
[3] Article 1 (a) of Directive 95/46/EC currently provides that 'personal data' shall mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social.identity." Recital (26) now states that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." The proposed Regulation therefore only introduces a definition of 'data subject' on the basis of existing elements.
[4] Opinion 4/2007 on the concept of personal data (WP 136)
[5] Wording in **bold** is an addition to the text. Wording between [….] is proposed to be deleted.

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 all 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"*.

The Working Party has already developed in its opinion 4/2007 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 an individual and treat that person in a specific way. [6]

The Working Party therefore suggests changing recital 24 accordingly.

Recital 24: '*When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify* ***or single*** *them* ***out****. It follows that identification numbers, location data, online identifiers or other specific factors as such* ***should as a rule be considered*** *[delete:need not necessarily be considered as] personal data [delete: in all circumstances].'*

[6] See also Preliminary FTC staff report "Protecting Consumer Privacy in an Era of Rapid Change", December 2010 and FTC report "Protecting Consumer Privacy in an Era of Rapid Change", March 2012.

On the notion of consent

The data subject's consent constitutes the first legal ground in Article 6(1) for the processing of personal data provided that certain conditions are met. These conditions are specified in Article 4 (8) and Article 7 of the proposed Regulation.

However, consent plays a role, where relevant, as part of a larger context where other grounds can also be used to legitimise the processing of personal data.

The recent opinion of the Article 29 Working Party on consent[7] insists on the need to ensure that consent is used in the right context, and is not misused. Where consent is used, it should be sufficiently clear. This can be expressed in different ways, for instance through a statement or an affirmative action, as the notion has sufficient flexibility built in. 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.

Building on the opinion of the Working Party, Article 7 of the draft Regulation introduces new and positive elements in particular by imposing the burden of proof on the controller, by introducing safeguards in the context of a written declaration and by excluding the validity of the consent where there is a significant imbalance between the position of the data subject and the controller. The Working Party very much welcomes these important clarifications and strengthening of the rights of individuals.

The Working Party understands that doubts have been raised as to the feasibility of the word "explicit" in the context of consent in Article 4 (8). The Working Party is of the opinion that the inclusion of the word "explicit" is an important clarification in the text, which is necessary to truly enable data subjects to exercise their rights, especially on the Internet where there is now too much improper use of consent. It would be highly undesirable should this important clarification be deleted from the text.

The Working Party finally emphasizes that the notion of consent has a general meaning in a wide range of situations. The conditions put forward in Article 4 (8) and Article 7 are in its view fully adequate to ensure an appropriate use of consent in all those situations. As to the specific case of cookies, the Working Party has recently highlighted the additional flexibility that has been provided in that context.[8]

[7] Opinion 15/2011 on the notion of consent (WP187)
[8] Opinion 4/2012 on cookie consent exemption (WP 194)

On the proposed delegated acts

In the proposal of the Commission for a new Regulation on data protection, a considerable amount of delegated and implementing acts is foreseen. While such further acts can in some instances be a valuable instrument for providing further harmonisation and guidance, the Article 29 Working Party has some reservations with regard to the extent the Commission would be empowered to adopt such acts, as also mentioned in its opinion regarding the data protection reform proposals (WP191). As mentioned above, both the LIBE committee of the European Parliament and the Council have expressed similar concerns and have announced they will examine the proposed delegated and implementing acts article by article to determine whether they are indeed needed.

The Working Party has in its opinion regarding the data protection reform proposals indicated that the European Data Protection Board (EDPB), the successor of the Working Party, should in any case be consulted in the process of drafting the delegated or implementing acts. Moreover, one of the main tasks of the Working Party nowadays is to provide interpretative guidance. The guidance provided the past years, mainly in the form of opinions, has proven its added value. In the future, it is even more important that the EDPB provides such interpretative guidance. As the EDPB consists of all EU national data protection authorities, it may in some situations even be in a better position to provide guidance.

Differences between delegated and implementing acts

Since the entry into force of the Lisbon Treaty the Commission can be empowered to adopt delegated acts and implementing acts. Delegated acts are based on article 290 TFEU and can be adopted to supplement or to amend non-essential parts of the legal act (in this case the proposed Regulation). Implementing acts are based on article 291 TFEU and can be used where uniform conditions are needed for implementing legally binding acts of the Union, such as a Directive or a Regulation.

With regard to delegated acts the proposed delegation of powers means that a substantial part of the rules will not be part of the proposed Regulation and will not be adopted through the normal legislative procedures. This does however not mean that the European Parliament and the Council will not be involved in adopting a delegated act. Delegated acts will only enter into force if the European Parliament and the Council do not object within 2 months after having been notified about the act, as also follows from Article 86 of the proposed Regulation.

If the European Parliament or the Council objects, this means that the delegated act will not enter into force. The Commission may then decide to propose a new delegated act taking into account the objections or can draft new legislation if the objection was based on exceeding the delegated powers. Another possibility of course is that the Commission decides not to propose any further acts or legislation.

Article 290 TFEU does not foresee a possibility for the European Parliament or the Council to propose amendments, they can only object to the entry into force of a delegated act.

Article 290 and 291 TFEU do not provide clear criteria for choosing between a delegated and an implementing act. From the proposed Regulation it becomes clear that the Commission considers implementing acts for ensuring the uniform, more technical conditions for the implementation of the Regulation, such as standard forms and standard procedures.

Inserting a power for the Commission to adopt delegated and implementing acts does not necessarily mean that the Commission is obliged to adopt all the acts proposed in the Regulation. Most of the acts will only be adopted when the need is felt to do so.

The Working Party underlines that the possibility for adopting delegated and implementing acts should only be inserted in cases where the Commission can substantiate that is indeed necessary. The fact itself that such an assessment cannot be made at the moment of the adoption of the Regulation in all cases, does not give sufficient justification for granting power to the Commission to adopt delegated or implementing acts, just in case.

It follows from the above that there are several ways for regulating data protection at the EU level:

- in the proposed Regulation itself;
- in a delegated act;
- in an implementing act;
- in the recitals of the Regulation.

However, a consistent and harmonised approach on EU level can in some cases be better achieved by interpretative guidance provided by the EDPB (which may include endorsing codes of conduct).

As the Commission seems to consider implementing acts mainly to be used for ensuring the uniform, more technical conditions for the implementation of the Regulation, such as standard forms and standard procedures and not so much for the further implementation and application of the (substantial) norms, these acts have for now been left out of the following assessment. Nevertheless, they may need to be analysed as well.

Assessment of proposed delegated acts

The Commission has made it clear from the outset that the aim of the reform was to ensure harmonisation and to ensure that the instrument remains technology neutral. Therefore when analysing the proposed delegated acts this aim has been taken into account.

Another clear criterion (stemming from Article 290 TFEU) is that essential elements should be dealt with in the basic act, i.e. the proposed Regulation, and not in a delegated act. The WP 29, as well as the EDPS, have indicated several provisions in the proposed Regulation in which powers were delegated to the Commission which concerned essential elements.[9]

Furthermore, it is in some instances important to ensure legal certainty. Laying down norms in binding EU instruments ensures legal certainty, as well as a level playing field within the EU. There are situations in which a binding EU instrument which specifies a provision of the Regulation will be the most appropriate way to create legal certainty, protect the data subject and avoid distorting discrepancies between the Member States.

However, in other situations a flexible approach and room for cultural differences might be more appropriate to ensure the practical application of the rules. In such cases it may be more suitable to provide guidance through guidelines of the EDPB, which acknowledges the need for flexibility and supports the introduction of the principle of accountability. Ultimately, the matter is left to the Court of Justice and national courts.

The choice to deal with a specific data protection issue in one or several of the instruments mentioned earlier should be made on the basis of clear criteria.

Criteria used for the assessment are:

- whether the issue concerns an essential part of the Regulation or not;
- whether the issue needs to be dealt with at European or national level (i.e. is there a the need for harmonisation);
- whether a legally binding or a more flexible instrument is needed;
- whether the instrument in compatible with the need for technological neutrality;
- whether there is a need to provide further guidance at all (i.e. whether or not it should be left to the controller to give substance to the rules under the specific circumstances of the case, subject always to supervision, enforcement and judicial review).

[9] Opinion 1/2012 (WP191), page 7 and EDPS opinion, pt. 74.

In the annex to this opinion, the articles in which delegated acts are proposed, are identified and analysed and an assessment has been made whether a delegated act would indeed be the most appropriate way for dealing with the issue(s) concerned. Other instruments considered next to a delegated act that could provide further guidance are:

- to deal with the issue in the text of the Regulation;

Instead of providing for a possibility to adopt delegated acts, some issues could, or should, be incorporated in the text of the Regulation itself. Further specifying some issues in the text of the Regulation would lead to harmonization because the Regulation is directly applicable across the EU. However, this could risk not being flexible enough to cover all possible situations and it would risk not being technologically neutral. Furthermore, trying to incorporate more rules into the Regulation itself might risk to slow down the reform process.

- to deal with the issue in a recital of the Regulation;

Certain issues could be dealt with in a recital of the Regulation, instead of in a delegated act. A recital can to some extent give helpful, general guidance on the purpose and *rationale* of a specific provision. However, trying to incorporate more examples in recitals of the Regulation might risk to slow down the reform process, or to give rise to bad law, driven by special interest and not by general principles.

- to leave it to national law;

To take into account (cultural, legal and historical) differences between Member States, further specification could also be provided by national law. This could however undermine the aim for harmonization and the functioning of the internal market.

- guidance by the EDPB;

Guidance by the EDPB may under certain circumstances be a good alternative to a delegated act. Guidance by WP29 is not a new instrument. Today, the Article 29 Working Party already provides opinions and recommendation on all matters relating to the protection of persons with regard to the processing of personal data following article 30 of the current Directive 95/46. By issuing joint opinions the current Article 29 Working Party contributes to a harmonized application of the current legal framework. Even though these opinions are not legally binding per se, they are authoritative and have proven their added value. Guidance from the EDPB is a flexible instrument that can relatively easily be adapted and revised or updated, for example following technical developments.

- not to provide any further guidance or legislation at all;

In some cases, not providing any further guidance or legislation could be proposed, because the provisions itself are clear enough for all stakeholders concerned and controllers themselves should ensure compliance with the Regulation, subject always to supervision, enforcement and judicial review.

ANNEX

Article 6(5) – for further specifying the conditions referred to in article 6(1)(f) for various sectors and data processing situations, including as regards processing of personal data related to a child.

Article 6 deals with the lawfulness of processing, by setting out six alternative legal bases of processing operations in Article 6 (a)-(f), *at least one of which* must be applicable at some stage.

Paragraph 1(f) provides that processing of personal data shall be lawful only if and to the extent that processing is necessary for purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

According to article 6(1)(f) a legitimate interest may be a legal ground for processing personal data, if, and to the extent in which, certain conditions have been fulfilled, requiring a balancing test to be executed, in the light of the circumstances of each case.

Following the accountability principle (which is dealt with in article 22 of the proposed Regulation) it should be left to the controller to decide whether it has a legitimate interest to justify certain data processing or whether such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This will be subject to supervision, enforcement and judicial review.

Nonetheless, since it regards one of the legal grounds for processing, providing further guidance is essential to have a common understanding of the provision. Further guidance on common criteria or examples for the concept of legitimate interest would be useful to ensure consistency in application and implementation.

Considering all different situations (in present and future) of what could constitute a legitimate interest and where such interests would be overridden by the interests or fundamental rights and freedoms of the data subject, a more flexible instrument seems more appropriate than a binding instrument.

It is moreover doubtful whether a delegated act would be an appropriate instrument to deal with this essential element of the Regulation.

Leaving further regulation to national law would lead to highly undesirable divergences in interpretation and application. Data controllers would be allowed to process data on the basis of this ground in one Member State and possibly not in another. To ensure consistency of

interpretation and application of this legal basis for processing, guidance should therefore be provided on a European level.

To allow for the necessary flexibility, instead of dealing with this issue in a delegated act, it would seem more appropriate that the EDPB issues guidelines regarding in which circumstances the ground 'legitimate interest' can be invoked and how to assess whether such interests are overridden by the interests or fundamental rights and freedoms of the data subject, amongst others by providing concrete examples.

Article 8(3) – for further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in the first paragraph. In doing so, the COM shall consider specific measures for MSMEs.

Article 8(1) provides that for the purposes of the Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

Following the accountability principle, it should be left to the controller to ensure it obtains verifiable consent, taking into consideration available technology.

Specifying the criteria and requirements for the methods to obtain verifiable consent in a legal document would also seriously risk not being flexible enough and may also unsufficiently meet the requirement of being technologically neutral.

Furthermore, allowing this issue to be regulated in national law would lead to differences between obligations put on controllers, thereby going against the aim of harmonisation and the creation of a level playing field, and would not bring the required flexibility.

In conclusion, there is already a clear obligation on the controller to make reasonable efforts to obtain verifiable consent, taking into consideration available technologies. It does therefore not seem necessary to provide further guidance in a delegated act.

With regard to the special consideration for MSMEs there does not seem to be a compelling reason why to do so. Especially since the reason for introducing this article is that children are vulnerable, it would seem odd to exclude MSMEs from having to obtain verifiable consent in case it regards personal data of children. Furthermore, a delegated act may never introduce exemptions for SME's that are not already foreseen in the text of the Regulation itself.

Article 9(3) – for further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data in article 9(1) and exemptions in article 9(2).

Article 9 deals with special categories of personal data and provides for a prohibition on processing the mentioned categories, except in the 10 exemptions set out in paragraph 2.

The article resembles the way in which the current Directive deals with special categories of data, which places a clear prohibition on processing special categories of data, but provides for some exemptions. As far as *criteria and conditions* are concerned, the current situation does not seem to lead to many problems, therefore specifying the criteria and conditions for the processing of special categories of personal data would not seem necessary.

As paragraph 1 and 2(a-f) of the article are already clear by generally prohibiting the processing of the mentioned special categories of personal data except in certain circumstances, there does not seem to be a need to further specify criteria and conditions.

Nonetheless, from past experience it appears that in some situations it would be useful to provide further guidance on what constitute appropriate safeguards.

Since establishing what constitute appropriate safeguards can only be done on a case by case basis, it would be impossible to provide further guidance in a legally binding document. Therefore a more flexible instrument would be most appropriate to provide further guidance on what could be appropriate safeguards.

Therefore, the EDPB could issue guidance on this issue. When possible, non-exhaustive examples could also be provided in a recital of the Regulation.

With regard to paragraph 2(g), the Regulation provides exemptions from the general prohibition for tasks carried out in the public interest. It would make sense that the controller makes the judgement whether or not the exemption can be used, subject always to supervision, enforcement and judicial review. However, the exemption would benefit from some further guidance to ensure harmonisation in application and consistency on the European level.

In view of the wide diversity of situations under which a data processing may be allowed based on the exemption for tasks carried out in the public interest, a delegated act does not seem to be the appropriate instrument. A more flexible instrument would be more useful to provide guidance to the controller on when, despite of the general prohibition, it can process personal data based on this exemption.

Furthermore and following the Article 29 Working Party opinion on the proposals it should be identified per article as much as possible what the specific public interests could be.

Considering the above, the specific public interests foreseen in article 9(2)(g) should be further clarified in the text of the Regulation itself and possibly further explained in a recital.

Article 12(5) – for further specifying the criteria and conditions for the manifestly excessive
requests and fees referred to in article 12(4).

Article 12 concerns specifically the fees to be charged when a request made by a data subject is manifestly excessive.

Article 12(4) provides that the information and the actions taken on requests by data subjects in exercising their rights shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In this case, the controller shall bear the burden of proving the manifestly excessive character.

The article provides in paragraph 4 that "...the controller shall bear the burden of proving the manifestly excessive character of the request". Following the accountability principle it should be left to the controller to assess whether the request is manifestly excessive. This will always be subject to supervision, enforcement and judicial review.

Since determining whether a request is manifestly excessive must always be done on a case by case basis, taking into account all circumstances, specifying the criteria and conditions in a more flexible instrument seems more appropriate.

With regard to the fees which can be charged in case a request is manifestly excessive, it would seem impossible or inappropriate to try to arrange this in a legally binding instrument or even at EU level, because this would not take into account the differences across Member States or across sectors.

In conclusion, there seems to be no need to provide for further legislation nor guidance with regard to the criteria and conditions for manifestly excessive requests and fees referred to in article 12(4). When deemed necessary however the maximum amount that can be charged could be regulated in national law.

Article 14(7) – for further specifying:
- the criteria for categories of recipients referred to in article 14(1)(f),
- the requirements for notice of potential access referred to in article 14(1)(g),
- the criteria for the further information necessary in article 14(1)(h) for specific sectors and situations, and
- the conditions and appropriate safeguards for the exceptions laid down in article 14(5)(b).
In doing so the Commission shall take appropriate measures for MSME.

Article 14 concerns the information to be provided to the data subject.

Paragraph 1 (f-h) provides that where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the recipients or categories of recipients of the personal data (f), where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission (g), and any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected (h).

Paragraph 5(b) provides that the first 4 paragraphs of article 14do not apply, where the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort.

The rights and obligations provided in the article are already quite clear. Especially compared to the current Directive 95/46 the article provides more clarity and guidance to the stakeholders concerned.

Furthermore, the responsibilities of the data controller should be taken into account, especially with regard to the criteria for categories of recipients referred to in article 14(1)(f), the requirements for notice of potential access referred to in article 14(1)(g) and the criteria for the further information necessary in article 14(1)(h) for specific sectors and situations.

With regard to the conditions and appropriate safeguards for the exceptions laid down in article 14(5)(b) the controller should also be able to assess and demonstrate whether providing information involves a disproportionate effort, subject to supervision, enforcement and judicial review.

Providing further guidance on what a disproportionate effort is would however be helpful, since it makes an exception to one of the basic rights of a data subject (right of information). This is especially an important right in cases where the controller did not collect the data directly from the data subjects.

To ensure harmonisation on this issue, further guidance should be provided at European level. Especially in today's interconnected world diverging interpretation of this exemption would have a serious impact on data subjects and controllers, and would not ensure harmonisation. This guidance could best be provided by the EDPB. For reasons of legal certainty, a binding instrument could be considered, only setting out conditions and safeguards on main lines.

The main conditions and appropriate safeguards for the exception of Article 14(5)(b) discharging the controller from providing the data subject with information could be developed in a delegated act. However, more detailed guidance from the EDPB could help with assessing in which cases controllers could make use of the exemption, based on an analysis of various practical situations and contexts.

Placing different (less stringent) obligations on controllers because of their size could seriously undermine the aim of the article, which is to oblige controllers to be transparent to allow data subjects to make informed choices. Therefore the obligation to provide the necessary information to allow the data subject to make an informed choice should be applicable despite the size of the controller. Furthermore, a delegated act may never introduce exemptions for SME's that are not already foreseen in the text of the Regulation itself.

Article 15(3) – for further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in article 15(1)(g).

Article 15 deals with the right of access for the data subject and 15(1)(g) specifically deals with the communication of the personal data undergoing processing and of any available information as to their source.

The issue to be further specified in the proposed delegated act relates to obligations on controllers, even though article 15 itself concerns the right of access of data subjects. In this respect, following the accountability principle, it should be left to the controller to ensure it complies with the law, subject always to supervision, enforcement and judicial review.

In addition, the right of the data subject is clear in that it provides that the data subject shall be provided with information on the personal data undergoing processing and of any available information as to their source.

Therefore it seems no further legislation or guidance is necessary.

Nb. What could however benefit from being further clarified is whether article 15(1)(g) indeed also means the actual personal data being processed, as can be inferred from paragraph 3.

Article 17(9) – for further specifying:
- the criteria and requirements for the application of article 17(1) (right to be forgotten) for specific sectors and in specific data processing situations; and
- the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in article 17(2) (informing 3rd parties); and
- the criteria and conditions for restricting the processing of personal data referred to in article 17(4).

Article 17 deals with the right to be forgotten.

Paragraph 1 provides that the data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed (a), the data subject withdraws consent or where the storage period consented to has expired and where there is no other legal ground for processing (b), the data subject objects to the processing of personal data pursuant to article 19 (c) or the processing of the data does not comply with the Regulation for other reasons (d).

The proposed delegated acts would further specify the requirements for the application of the right to be forgotten for different sectors or processing operations, the conditions for deleting links, copies and replications, and restrictions of processing operations.

To ensure a harmonised interpretation and implementation of article 17, it would be beneficial to provide further guidance on European level, so that both data subjects and controllers know what their rights and obligations are across the EU.

Since the Regulation itself cannot adequately adress all relevant situations, further guidance should be provided by a different instrument.

In order to ensure legal certainty for data subjects and data controllers, the application of the right to be forgotten for different sectors or processing operations, the conditions for deleting links, copies and replications and the restrictions of processing operations should be dealt with in a legally binding document.

Therefore a delegated act indeed seems to be the most appropriate manner, provided it will be adopted at the same time as the Regulation enters into force.

Article 20(5) – for further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in article 20(2) (exceptions to prohibition on profiling).

Article 20 deals with profiling and the second paragraph provides that subject to the other provisions of the Regulation, a person may be subject to profiling if the processing is carried out in the course of entering into, or performance of, a contract, where the request for the entering into or the performance of a contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention (a), is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests (b) or is based on the data subject's consent (c).

Article 20(1) provides that "Every natural person shall have the right not to be subject to a measure which produces legal effects ... or significantly affects this natural person ... intended to evaluate certain personal aspects ... or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliabiltity, behaviour." The second paragraph provides for three exemptions from this right.

The issue that the proposed delegated act(s) intend(s) to cover seems to relate to the obligation on the controller to determine whether it can subject an individual to the measures referred to in article 20(1) on the basis of the data subjects' legitimate interests, despite its general prohibition.

Since a controller cannot always determine what kind of measures are suitable measures to safeguard the legitimate interest of a data subject and since the provision regards an exception to a right of the data subject who is entitled to legal certainty, a legally binding instrument seems most appropriate. To avoid fragmentation and to ensure the same level of protection for all individuals further specification should be provided on a European level.

A delegated act could therefore be an appropriate instrument, provided the delegated act will be adopted at the same time as the Regulation enters into force. Additionally, it could also be suitable for the EDPB to issue further guidance on the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests.

Article 22(4) – for further specifying:
- any further criteria and requirements for appropriate measures referred to in article 22(1) other than those already referred to in article 22(2);
- the conditions for the verification and auditing mechanisms referred to in article22(3); and
- as regards the criteria for the proportionality under article 22(3) and considering specific measures for MSMEs.

Article 22 is the so-called "general accountability article" and provides in the first paragraph that the controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. Paragraph 2 provides what these measures shall in particular include and the third paragraph provides that the controller shall implement mechanisms to ensure the verification of the effectiveness of the measures. If appropriate this verification shall be carried out by independent internal or external auditors.

Article 22 sets out the obligation on controllers to ensure compliance and is based on the accountability principle. According to this principle, what policies and measures the controller adopts to ensure and be able to demonstrate compliance with the Regulation should be left to the controller, as long as they are both appropriate and effective. This will always be subject to supervision, enforcement and judicial review.

Since the second paragraph of the article already provides non-exhaustive examples of how to give substance to the general obligation, there seems to be no need to even further specify additional criteria and requirements.

Implementing mechanisms to ensure verification of the effectiveness of the measures adopted, should also be left up to the controller, because it depends on the sector or business model what mechanism would be most suitable.

In conclusion, since the article itself gives substance to the accountability principle, there seems to be no need to specify any further the criteria and requirements for appropriate measures other than those already provided in paragraph 2 and the conditions for the verification and auditing mechanism.

With regard to special consideration to MSMEs, the general obligation to be accountable and to adopt policies and implement appropriate measures to ensure and be able to demonstrate compliance should apply regardless of size of the controller. Though of course MSMEs should be allowed to adopt such mechanisms and measures scalable. Furthermore, a delegated act may never introduce exemptions for SME's that are not already foreseen in the text of the Regulation itself.

.

Article 23(3) – for further specifying criteria and requirements for appropriate measures and mechanisms referred to in article 23(1)&(2), in particular for data protection by design requirements applicable across sectors, products and services.

Article 23 concerns the principles of data protection by design and by default.

Considering the accountability principle of article 22 it should be left to the controller to determine which appropriate technical and organisational measures and procedures to implement to ensure compliance with the principles of data protection by design and by default.

Furthermore, the obligation on controllers in article 23 is already quite clear as it puts the responsibility of implementing appropriate measures and procedures on the controller.

As it can only be assessed on a case-by-case basis whether or not the controller has taken the appropriate measures and procedures, having regard to the state of the art and cost of the implementation, it seems close to impossible to cover all situations in the Regulation.

In conclusion, no further legislation or guidance seems necessary. However guidance issued by the EDPB may be useful.

Article 26(5) – for further specifying:
- the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with article 26(1); and
- conditions which allow facilitating the processing of personal data within a group undertakings, in particular for the purposes of control and reporting.

Article 26(1) provides that where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organisational measures governing the processing to be carried out and shall ensure compliance with those measures.

It seems there is no need to further specify the criteria and requirements for the responsibilities, duties and tasks in relation to a processor, nor to further specify the conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting, considering the requirements already provided by the Regulation, especially in terms of accountability of the controller.

There is an obligation on controllers to ensure that the processor provides sufficient guarantees in such a way that the processing will meet the requirements of the Regulation. In addition, the second paragraph of the article already specifies which aspects shall be covered by the contract or other binding document.

Furthermore, as many different factors can influence the relation between a controller and a processor, how to give substance to this obligation needs to be assessed on a case by case basis.

With regard to further specifying conditions which allow facilitating the processing of personal data within a group of undertakings, this should also be left to the controller following the principle of accountability, considering there already is an obligation to ensure in a binding contract that the processing operation meets the requirements of the Regulation

Moreover, when data is exchanged with parts of an undertaking outside the EEA, the possibility of using a BCR is already provided in the Regulation.

Considering the above no further legislation or guidance is necessary.

Article 28(5) – for further specifying the criteria and requirements for the documentation referred to in article 28(1), to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

Article 28 concerns the obligation on controllers to maintain documentation.

Following the accountability principle it would seem appropriate to leave it to the controller, processor and the representative how precisely to ensure compliance with the documentation.

Furthermore, the second paragraph of article 28 already provides for a non-exhaustive list of what should at least be documented. **There does not seem to be a need to even further specify the criteria and requirements.**

Article 30(3) – for further specifying the criteria and conditions for the technical and organisational measures referred to in article 30(1)&(2), including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of the developments in technology and solutions for privacy by design and data protection by default, unless article 30(4) applies (implementing acts).

Article 30 concerns the security of processing

Following the accountability principle it should be left to the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by the processing and nature of the personal data to be protected, taking into account the state of the art and the costs of the implementation.

Further specifying the criteria and conditions for the technical and organisational measures would not be able to cover all different situations between sectors and processing operations.

One of the aims of the review of the data protection legal package is to remain technology neutral. The proposed delegated acts however would also specify further the determinations of what consitutes the state of the art. Even though a delegated act itself may be not technologically neutral, it may be inappropriate to lay down in a legally binding instrument what constitues the state of the art. It would furthermore seriously run the risk of being outdated when adopted.

Therefore, further specification by adopting a delegated act does not seem appropriate. However further guidance by the EDPB could be foreseen where necessary.

Article 31(5) – for further specifying the criteria and requirements for establishing a data breach referred to in article 31(1)&(2) and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

Article 31 concerns the obligation on the controller to notify a personal data breach to the supervisory authority.

Paragraph 1 provides that in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.

Paragraph 2 provides that pursuant to article 26(2)(f), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

The proposed delegated act relates to the criteria and requirements for establishing a data breach and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

Providing guidance on the criteria and requirements for establishing a data breach and the particular circumstances in which a breach shall be notified is indeed important, it should be made clear what amounts to a personal data breach.

To ensure a harmonised implementation and application of the obligation to notify a personal data breach to the supervisory authority, further guidance should be provided on a European level.

Considering its importance for all stakeholders concerned it is important to provide clarity in a legally binding text and since it is an essential part of the rules and obligations, it should be dealt with in the text of the Regulation itself.

Therefore instead of further specifying the criteria and requirements for establishing a data breach and the circumstances under which it should be notified in a delegated act, at least the main lines should be made clear in the text of the Regulation.

It would be desirable to provide for certain details in a delegated act, provided it is adopted at least at the same time as the Regulation enters into force.

Article 32(5) – for further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in Article 32(1).

Article 32 concerns the obligation on the controller to communicate the personal data breach to the data subject.

Paragraph 1 provides that when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification to the supervisory authority, communicate the personal data breach to the data subject without undue delay.

The proposed delegated act relates to the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect (the protection of) the personal data or privacy of the data subject.

Providing guidance on the criteria and requirements as to the circumstances in which a personal data breach is likely to have such an adverse effect is indeed important. It should be made clear what conditions require a communication to the data subject.

To ensure a harmonised implementation and application of the obligation to communicate a personal data breach to the data subject, further clarity should be provided on a European level.

Considering its importance for all stakeholders concerned it is important to provide clarity in a legally binding text, and since it is an essential part of the rules and obligations, it should be dealt with in the text of the Regulation itself.

Therefore instead of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to have an adverse effect and should be communicated to the data subject in a delegated act, this should - at least on main lines - be made clear in the text of the Regulation.

It could be desirable to provide for certain details in a delegated act, provided it is adopted for the first time before the Regulation enters into force.

Article 33(6) – for further specifying:
- the criteria and conditions for the processing operations likely to present specific risks referred to in article 33(1)&(2); and
- the requirements for the assessment referred to in article 33(3), including conditions on scalability, verification and auditability.
In doing so the COM shall consider specific measures for MSMEs.

Article 36 concerns the obligation to carry our data protection impact assessments.

The first paragraph provides that where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Paragraph 2 provides for 5 processing operations that in particular present specific risks.

Paragraph 3 provides that the assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure protection of personal data and to demonstrate compliance with the Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

Controllers shall carry out a data protection impact assessment when a processing operation is (likely) to present specific risks to the rights and freedoms of data subjects by virtue of their nature, scope and purposes. Following the accountability principle it should be left to the controller to determine whether the processing operations (are likely to) present specific risks to the rights and freedoms of data subjects.

However, this is an important issue, which as an impact on whether or not a controller is obliged to carry out a data protection impact assessment and whether it presents specific risks to the rights and freedoms of data subjects. Consistency at European level is important to ensure a harmonized interpretation and application of the article.

General requirements on how to assess whether or not a processing operation presents specific risks may be laid down in a delegated act. Alternatively or additionally, further guidance by the EDPB could be foreseen , provided that any possible list of processing operations that would be identified as presenting specific risks shall not be exhaustive.

With regard to the special consideration for MSMEs there does not seem to be a compelling reason why to create a special position for them. Especially since the purposes of the article is to have additional safeguards when a processing operation (is likely to) presents specific risks to the rights and freedoms or the privacy of data subjects, it should not exclude controllers because of their size from this obligation. Furthermore, the article itself already

provides for a threshold with the phrase "(are likely to) present specific risks...", which is an exemption based on the nature of the processing, which makes more sense that an exemption on the basis of the number of employees. Furthermore, a delegated act may never introduce exemptions for SME's that are not already foreseen in the text of the Regulation itself.

Article 34(8) – for further specifying the criteria and requirements for determing the high degree of specific risk referred to in article 34(2)(a) (prior consultation after a DPIA).

Article 34 concerns the obligation on controllers to seek prior authorisation or consultation from the supervisory authority. Article 34(2)(a) specifically deals with the obligation on controllers to consult the supervisory authority prior to the processing of personal data in order to ensure compliance of the intended processing with the Regulation and in particular to mitigate the risks involved for the data subject when a data protection impact assessment indicated processing operations are by virtue of their nature, their scope or their purposes likely to present a high degree of specific risks.

The proposed delegated act(s) would further specify the criteria and requirements for determining the high degree of specific risks presented by a processing operation, following a data protection impact assessment.

While it would seem appropriate to leave it to the controller to decide whether the risks identified after having carried out a DPIA are of a high degree or not, this relates to the risks to a data subject's data or privacy, which means it is important to provide further guidance. To ensure a harmonized approach in the EU, the criteria and requirements should be further specified on a European level.

Since all processing operations are different whether or not there is a high degree of specific risks would depend on the merits of the case. Dealing with all possible situations in a legally binding document is almost impossible, therefore a more flexible instrument seems appropriate.

Furthermore, since the supervisory authorities must deal with the requests for prior authorisation and consultation, it would be most appropriate to have the EDPB issue guidelines, all the more since the EDPB is already involved in cases where prior consultation is deemed necessary by the authorities.

In conclusion, instead of a delegated act, guidelines from the EDPB would be most appropriate to further specify the criteria and requirements for determining the high degree of specific risks (likely to be) presented by processing operations, following a data protection impact assessment.

Article 35(11) – for further specifying:
- the criteria and requirements for the core activities of the controller or the processor referred to in article 35(1)(c); and
- the criteria for the professional qualities of the DPO referred to in article 35(5).

Article 35 provides an obligation for controllers and processors to designate a data protection officer in any case where the processing is carried out by a public body or authority (1)(a); the processing is carried out by an enterprise employing 250 persons or more (1)(b); or the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects (1)(c).

Article 35(5) provides that the controller or processor shall designate the DPO on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.

One of the proposed delegated acts would specify further the criteria and requirements for the core activities of the controller or the processor consisting of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

To ensure a harmonised interpretation and application of Article 35, further rules on European level would be beneficial. Laying these rules down in a legally binding document could cover different situations at least in main lines, although probably not all situations.

A delegated act setting out main lines would be an appropriate instrument. Additionally, guidance from the EDPB could help with further specifying the criteria and requirements for the core activities of a controller or processor requiring monitoring of data subjects.

A delegated act is also proposed to further specify the criteria for the professional qualities of the DPO.

Further to the accountability principle, it should at least to some extent be left to the controller or processor to assess the qualities of a DPO. It greatly depends on the sector and business model what the qualities of a DPO should be. However, widely divergent approaches of this subject between different MS - either or not at sector level - would seriously undermine the level playing field and mutual trust aimed at in the proposed Regulation.

In conclusion, it would be appropriate for a delegated act to further specify the criteria for the professional qualities of the DPO on main lines. Additional guidance could be provided by the EDPB.

Article 37(2) – for further specifying the criteria and requirements for tasks, certification, status, powers and resources of the DPO referred to in article 37(1).

Article 37 deals with the tasks of the DPO and the first paragraph sets out which tasks the controller or processor shall at least entrust the DPO with.

The general obligation in Article 37(1) is already quite clear as it puts the responsibility of ensuring that certain tasks are entrusted to the DPO on the controller and the processor. In addition, the list with tasks in paragraph 1 already specifies which tasks the DPO should at least be entrusted with.

Further to the accountability principle, it should at least to some extent be left to the controller or processor to further determine the conditions under which a DPO should be active. It may depend on different factors what those conditions should be.

However, widely divergent approaches of this subject between different MS - either or not at sector level - would once again seriously undermine the level playing field and mutual trust aimed at in the proposed Regulation. Moreover, these conditions will also influence the independent position of DPOs.

In conclusion, it would be appropriate for a delegated act to further specify the tasks, certification, status, powers and resources of the DPO referred to in Article 37(1) on main lines. Additional guidance could be provided by the EDPB.

Article 39(2) – for further specifying:
- the criteria and requirements for the data protection certification mechanisms referred to in article 39(1), including conditions for granting and withdrawal; and
- requirements for recognition within the Union and in third countries.

Article 39 provides that the Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors.

Considering that the trustworthiness of data protection certification mechanisms, seals and marks is highly dependable on the criteria and requirements set for establishing them, it is important to provide further guidance.

Since the certification mechanisms are to be encouraged in particular at European level, specifying further the criteria and requirements should be done on a European level as well.

Since it would be hard to spell out all criteria and requirements in full in the text of the Regulation, it would be appropriate to adopt a more flexible instrument to provide further criteria and guidance for the data protection certification mechanisms, including conditions for granting and withdrawal and for requirements for recognition within the Union and in third countries.

In order to ensure legal certainty towards the data subjects who rely on the certification mechanisms, seals and marks, a delegated act would indeed seem the most appropriate instrument.

Article 43(3) – for further specifying:
- the criteria and requirements for binding corporate rules within the meaning of this article, in particular as regards the criteria for their approval;
- the application of article 43(2)(b,d,e&f) to binding corporate rules adhered to by processors; and
- on further necessary requirements to ensure the protection of personal data of the data subject concerned.

Article 43 concerns international transfers by way of binding corporate rules. Paragraph 2 (b,d,e&f) indicate that BCRs should at least specify the data transfers or set of data transfers (b), the general data protection principles, measures to ensure data security and the requirements for onward transfers to organisations which are not bound by the policies (d), the rights of data subjects and the means to exercise these rights (e) and the acceptance by the controller or processor established on the territory of a Member State of liability of any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union (f).

First of all delegated acts are foreseen to further specify the criteria and requirements for binding corporate rules within the meaning of the article in general and in particular as regards the criteria for their approval. The first paragraph however already sets out that it is up to the supervisory authority in accordance with the consistency mechanism in article 58 to approve binding corporate rules. The same paragraph also provides some requirements that the supervisory authority shall take into account.

It seems that this already puts in place enough checks and balances to ensure that a BCR covers all aspects it needs to cover. Furthermore, considering that the consistency mechanism should be used when approving a BCR, there is already involvement at European level.

Moreover, it is the task of the supervisory authorities to approve the BCRs. Delegated acts on further specifying the criteria and requirements in general and in particular for their approval would risk encroaching upon the independence of the supervisory authorities and the EDPB.

Therefore there does not seem to be a need to further specify the criteria and requirements for binding corporate rules in general and in particular regarding the approval.

Secondly, delegated acts are foreseen for further specifying the application of article 43(2)(b,d,e&f) to binding corporate rules adhered to by processors. Considering it concerns critical issues that must be dealt with in a BCR, it would be beneficial to provide further harmonisation.

Since a BCR will be applicable across the EU, a harmonized application and interpretation should be ensured.

Considering that each BCR depends on the business model of a company and the sector in which it operates, it is close to impossible to deal with all situations in the Regulation itself. Therefore a more flexible instrument could be used.

A delegated act would be an appropriate instrument. Additionally, as the EDPB will be involved in the process following from the obligation to use the consistency mechanism for approving BCRs it would make sense for the EDPB to issue guidance on the application of the articles to binding corporate rules adhered to by processors.

Thirdly, delegated acts are proposed on further necessary requirements to ensure the protection of personal data of the data subject concerned.

Further to the accountability principle it should be left to the controller or processor itself to ensure compliance with the law, always subject to supervision, enforcement and judicial review. In addition, the article seems already clear in spelling out how a BCR shall be approved, by whom, according to which criteria and what should at least be covered by the BCR.

It is the role of the supervisory authorities to approve the BCRs and when necessary take enforcement actions, therefore delegated acts on further necessary requirements to ensure the protection of personal data of the data subject concerned would seriously risk encroaching upon the independence of the supervisory authorities.

As the EDPB will be involved in the process following from the obligation to use the consistency mechanism for approving BCRs, it would make sense for the EDPB to issue guidance on the application of the articles to binding corporate rules adhered to by processors.

Article 44(7) – for further specifying:
- 'important ground of public interest' within the meaning of article 44(1)(d); as well as
- criteria and requirements for appropriate safeguards referred to in article 44(1)(h).

Article 44 concerns derogations from the general prohibition to transfer personal data to third countries and international organisations.

Paragraph 1(d) provides that a transfer or a set of transfers of personal data to a third country or an international organisation may take place on the condition that the transfer is necessary for important grounds of public interests.

Paragraph 1(h) provides that a transfer or a set of transfers of personal data to a third country or an international organisation may take place on the condition that the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

Delegated acts are proposed to further specify what constitutes 'important ground of public interest' in regard of a derogation of the general prohibition on transferring personal data to third countries or international organisations. The specification of an 'important ground of public interest' concerns an essential element determining the lawfulness of data transfers, and should therefore be dealt with in the Regulation itself.

To ensure a harmonised application in the EU, this specification should be done in the text of the Regulation itself.

Delegated acts are also foreseen to further specify criteria and requirements for appropriate safeguards referred to in article 44(1)(h).

The Working Party would like to stress the need for further specifying the term "legitimate interest" in article 44(1)(h) in the Regulation as also mentioned with regard to the proposed delegated act in article 6(5). Such guidance could be given by respective EDPB guidelines, alternatively or additionally, a non-exhaustive list of examples of "legitimate interests" could be provided for in a recital of the Regulation.

With regard to what would be appropriate safeguards, further guidance seems important, since it concerns a derogation from a general prohibition to transfer data to third countries or international organisations, based on a legitimate interest and without involvement of a supervisory authority, further guidance seems important.

It would however be impossible to cover all different situations (in present and future) of what the appropriate safeguards would be in the Regulation itself. Therefore a more flexible instrument would be more appropriate.

To ensure harmonisation of interpretation and application, a delegated act would therefore seem to be an appropriate instrument. Additionally, the EDPB could issues guidance to further specify what constitutes appropriate safeguards in article 44(1)(h).

Article 79(7) – for updating the amounts of administrative fines referred to in article 79(4,5 & 6), taking into account the criteria referred to in article 79(2).

Article 79 concerns administrative sanctions. Paragraphs 4, 5 and 6 determine the maximum heights of the fines and paragraph 2 provides that the administrative sanction shall be in each individual case effective, proportionate and dissuasive and provides further criteria for determining the height of the fine.

Considering that the new legal package should be applicable for at least a few decades it is important to allow indexation of the fines and so to allow for adaptations to the amounts of fines in the future.

To avoid differences between the Member States and to ensure a harmonised maximum level in the EU, these updates should be provided on an EU level.

To ensure clarity to all stakeholders concerned a legally binding instrument should be used.

Therefore delegated acts for updating the amounts of administrative fines in paragraphs 4, 5 and 6 of article 79, taking into account the criteria in paragraph 2 of the article seem to be appropriate.

Article 81(3) – for further specifying the reasons of public interest in the area of public health as referred to in article 81(1)(b); as well as
- criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in article 81(1).

Article 81 provides that within the limits of the Regulation and in accordance with article 9(2)(h), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests and be necessary for the purpose of preventive or occupational medicine (a) or for reasons of public interest in the are of public health (b) or for other reasons of public interest in areas such as social protection (c).

The proposed delegated act(s) would deal with further specifying the reasons of public interest in the area of public health, as well as the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in article 81(1).

What constitute reasons of public interest in the area of public health, and what the criteria and requirements for the safeguards are, should be provided in a binding legal act. Considering it is impossible to provide such specific details in the text of the Regulation itself, a different instrument would be more appropriate.

Article 81(1) however leaves it to some extent to the Member States to provide for the lawfulness of data processing in the health sector in national law.

Therefore, delegated acts would seem the most appropriate instruments, subject however to article 81(1).

Article 82(3) – for further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in article 82(1).

Article 82 concerns data processing in an employment context.

The proposed delegated act(s) would deal with further specifying the criteria and requirements for the safeguards for the processing of personal data in the employment context.

Further criteria and requirements for the safeguards of processing personal data in this context, should be provided in a binding legal act. Considering that it is impossible to provide such specific details in the text of the Regulation itself, a different instrument would be more appropriate.

Article 82(1) however leaves it to some extent to the Member States to provide for the lawfulness of data processing in the employment context in national law.

Therefore, delegated acts would seem the most appropriate instruments, subject however to article 82(1).

Article 83(3) – fo further specifying:
- the criteria and requirements for the processing of personal data for the purposes referred to in article 83(1&2); as well as
- any necessary limitations on the rights of information to and access by the data subject; and
- detailing the conditions and safeguards for the rights of the data subject under these circumstances.

Article 83 concerns processing for historical, statistical and scientific research purposes.

Paragraph 1 provides that within the limits of the Regulation, personal data may be processed for historical, statistical or scientific research purposes only if these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject (a) and if data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner (b).

Paragraph 2 provides that bodies conducting historical, statistical or scientific research may only publish or otherwise publicly disclose personal data if the data subject has given consent (a), the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests of the fundamental rights and freedoms of the data subject do not override these interests (b) or the data subject has made the data public (c).

Delegated acts are proposed to further specify the criteria and requirements for the processing of personal data for historical, statistical and scientific research purpose if it fulfils the criteria and requirements in paragraphs 1 and 2.

The criteria set in the article are already quite clear in that it provides that the data may only be processed for historical, statistical and scientific purposes if it fulfils the two conditions mentioned. In all other cases it is prohibited. These criteria are essential elements in determining the lawfulness of processing.

If additional requirements must be met to be able to process data for historical, statistical and scientific purposes, these requirements should be provided in the text of the Regulation itself, to ensure a harmonised practice and legal clarity and certainty for all involved stakeholders.

With regard to the proposed delegated acts for further specifying any necessary limitation on the rights of information to and access by the data subject and those proposed for detailing the conditions and safeguards for the rights of the data subject under these circumstances, it is unclear where the possibility to limit these rights is provided (not in articles 14 and 15 either). In any case, as this is an essential element, it should be in the Regulation itself.

If there is a possibility for bodies conducting historical, statistical or scientific research to limit the rights of the data subject, this should be dealt with in a legally binding document to ensure clarity and certainty for the data subjects.

Therefore it should either be fully dealt with in the text of the Regulation itself or be further specified in a delegated act which is adopted at the time the Regulation enters into force.

Further guidance, where necessary, could be provided by the EDPB, or be laid down in an EU wide code of conduct.