COUNCIL OF THE EUROPEAN UNION

Brussels, 21 November 2012

15703/4/12 REV 4

Interinstitutional File: 2012/0011 (COD)

LIMITE

DATAPROTECT 122
JAI 752
DAPIX 137
MI 678
FREMP 131
DRS 121
COMIX 608
CODEC 2555

NOTE

from:	General Secretariat
to:	Working Group on Information Exchange and Data Protection (DAPIX)
No. Cion prop.:	5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Replies to the questionnaire on administrative burdens

The annex sets out a compilation of the replies to Annex I to 12918/1/12 REV 1 DATAPROTECT 97 JAI 551 MI 515 DRS 101 DAPIX 94 FREMP 110 COMIX 460 CODEC 1978, received at 14 November 2012.

Below are a number of general remarks which have been made by Member States:

GENERAL REMARKS

BELGIUM

The questions cannot be properly answered until other key issues have been addressed, in particular the degree of flexibility to be afforded to the public sector in applying European legislation. Any replies given now are merely provisional pending an agreement on the other elements of the enacting terms. Independently of its reply therefore, Belgium is maintaining its general reservation on the Commission proposal.

- In general, Belgium considers that the draft Regulation, notably Chapter IV, imposes disproportionate administrative burdens which are not compensated for by the removal of the notification requirement..

- The logic underlying Annex I to the Presidency's questionnaire is that, if the obligation laid down in the Regulation is disproportionate, the solution could be to limit the scope of the obligation based on certain criteria (size of the entity, risks, volume of data processed, number of persons affected, data categories). Nevertheless, Belgium believes that compliance with the principle of proportionality does not depend on the scope of application alone but also on the actual extent of the obligations. Belgium's reply is based on this approach.

CZECH REPUBLIC

CZ would like to thank the CY PRES for focusing on administrative burdens and compliance costs horizontally. CZ believes strongly that regulation should not undercut economic recovery and harm competitiveness of advanced and innovative European industries. As an introductory comment, CZ would like to indicate that a general discussion based on results of this questionnaire could yield prospective solutions. Especially if interconnections between identified administrative burdens and compliance costs and other provisions are taken into account, such general discussion might offer alternatives that might be more appropriate – such as simple rules for “small processing”, “risky processing” approach etc.

DENMARK

Denmark welcomes the opportunity to comment on the question of administrative burdens in connection with the Commission proposal on the General Data Protection Regulation. We would point out, however, that in Denmark's view there are more provisions than are apparent from the Presidency's draft which to some extent impose administrative burdens and which should for that reason be included in discussions. We would further point out that the question of the extent to which administrative burdens are proportionate cannot in every case have a simple "yes" or "no" answer.

The question of administrative burdens is in Denmark's view a very important one, and generally speaking for us it is absolutely vital that the administrative expenses imposed by the proposed regulation on both public authorities and private undertakings should be brought down. It is important that the administrative burdens which the proposal entails should be proportionate and therefore sufficiently offset by benefits, including rights and advantages, for the data subject or others. Denmark believes that such proportionality is to be achieved via a "risk-and-context-based approach".

The broad scope of the proposed regulation implies that it would apply both to general processing and to high-risk processing of personal data, and that in most cases it would be the same rules which would apply. This is not desirable, and it therefore needs to be considered whether the application of the rules in the proposal should be differentiated entirely according to the risk entailed by the data processing operation concerned. The criteria for evaluating whether or not a processing operation is risky can for example be laid down in a provision of the regulation.

The number of employees in the undertaking/authority may in many cases be a relevant factor to be taken into account in judging whether or not it is reasonable to impose an administrative burden and whether that burden is proportionate. In other cases, however, it will be more relevant to take account for example of the number of data subjects affected, the volume of data or the category of data subjects concerned. The decision as to whether a burden is proportionate depends on the specific view taken of the particular provision in each individual case, taking into account the relevant factors.

GERMANY

General comments from Germany

1. Germany welcomes the horizontal discussion on the issue of administrative burdens, which is a common thread running through the whole draft Regulation. In our opinion the key to solving this problem lies in attaching greater significance to the relative risk of a data processing operation, in particular by reducing the burden for low-risk data processing operations and providing for specific safeguards for high-risk data processing operations, which need to be defined more precisely. Discussion should concentrate on the definitions necessary for this, and on the question of which reductions are meaningful and appropriate for data processing operations with a lower risk, and which additional safeguards are necessary for operations with a high risk, with regard to which requirements in the draft Regulation. The aim should be to pinpoint as quickly as possible which specific obligations entail a disproportionate burden that needs to be reduced.

2. The draft Regulation therefore needs to be examined to determine whether, when taken as a whole, there is an appropriate balance between the data subjects' protection interests and the administrative burden. This burden should in particular be contained for data processing operations that can in general be regarded as posing a lower risk. Even though the administrative burden often does concern SMEs, focusing on the number of employees alone is not a suitable response to the questions of whether a data processing operation should be considered as high-risk or not and whether the personal data protection procedures proposed in the draft are appropriate. This is also the case for the public sector in particular. In addition, legal requirements in the public sector need to be taken into account, in particular regarding procedural rules and data subjects' obligation to cooperate.

3. We feel that the risk criteria listed in the questionnaire are not yet sufficient for a risk assessment. The volume of data and the number of data subjects can each be regarded as an indicator for an existing risk.

4. Further criteria should be developed to accompany those listed in the questionnaire. For this reason, we feel that the last column of the questionnaire ("other criteria") needs to be examined comprehensively with a view to developing further risk criteria for the provisions listed.

5. In our opinion, the prospect of incorporating a horizontal provision at an appropriate point in the general part of the draft Regulation should be discussed. Further risk determination criteria could be listed in that article. The article could then serve as a connecting factor for consequences in law, the implementation of which involves a high administrative burden. The following criteria could be used in the horizontal standard as indicators for a high-risk data processing operation:

   – sensitivity of the data due to their content (general examples, e.g. health-related personal data);
   – particular legitimate expectations due to the context of data collection and/or processing (e.g. the user has a justified expectation for their privacy to be particularly protected, for instance when using search engines, email programs or databases);
   – secret data collection and processing;
   – particularly intensive data processing, for instance due to the intended purpose (profiling);
   – a heightened risk of prohibited processing (large number of people authorised to access or receive the data, or connection possibilities, for example);
   – particularly prejudicial effects (e.g. irreversible, potentially discriminatory, severe infringements of privacy or personal honour); or
   – processing of a child's data.

6. In the case of certain obligations, a distinction should also be made according to areas of responsibility. For instance, direct obligations (regarding privacy by design and privacy by default, for example) should be imposed on information service providers and, if applicable, software and hardware manufacturers. At the same time, users and/or consumers could be exempted from certain responsibilities and burdens. Where no distinction is made between

data providers and consumers, these should often be simultaneously regarded as controllers, each with the same obligations.

7. The exact assessment of the administrative burdens must be based on reliable criteria and procedures (including the necessary involvement of those who have to bear the burden), which will take a considerable amount of time to define. For this reason, and because we believe that the Commission's estimation of the administrative costs is not yet complete, the answers to the questionnaire can only be treated as rough estimates. Moreover, the "Yes/No" options set out in the questionnaire only allow for black and white answers, so on that basis, a differentiated treatment of the various provisions is almost impossible. Germany therefore reserves the right to submit further comments.

8. When answering the questionnaire, we have described the provision in question as "disproportionate" when, in our opinion, the necessary criteria for further differentiation (e.g. risk approach or nature of the data) and/or (further) exceptions are lacking. Therefore the notion of proportionality is not used in the strictly legal sense of the word here.

ESTONIA

Please be informed that in the table below we present only those provisions where the administrative burden is disproportionate from our point of view. We would like to stress that the analysis below is our preliminary opinion and could change during the negotiations and after the amendments in the text of the draft regulation. We analyzed only the provisions that have already been discussed in the working party. We cannot give any opinion on the articles that have not been discussed yet. However, we consider it important to continue the discussion on this issue later on.

We evaluated the administrative burden on the following criteria:

- does the draft law influence the obligation of the enterprises, non-profit organizations or citizens to provide information to the public authorities and costs that can be involved, including raise of the information to be collected, inserted or controlled, also working procedures?
- does the draft law increase the obligations of the enterprises to request permits, opinions etc. from the public authorities or does the draft law increase the quantity of the working procedures and concomitant costs?
- does the draft law influence the obligations that are connected to the working procedures or does the draft law impose an obligation to implement new or specific technologies?

Generally, in most cases, we do not consider the size of the entity a suitable criterion. Therefore, from our point of view mainly the risk-based approach should be taken. The amount of data processed, the sensibility of the data and number of data subjects concerned is more valid criteria to assess the administrative burden. In case the sensitive data or a data of the child is processed, some additional requirements may be proportionate. We also encourage more flexibility and welcome provisions for self-regulation in non-essential issues or where no sensitive data is concerned. However, we welcome any further discussion on the administrative burden.

SPAIN

1. General Remarks

We would like to convey our genuine appreciation to the effort being done by the presidency in order to address the horizontal issues relating to the draft regulation on general data protection.

The Spanish delegation fully supports this initiative, which is in line with the explicit mandate issued by the Ministers, and is willing to continue collaborating constructively to resolve all outstanding issues.

In order to do so, we would like to make some general and previous remarks for the sake of the discussion ahead.

1. General remarks on the questionnaire

"Administrative burdens" is a very serious issue. On one hand bureaucratic burdens can be seen on the basis of the guarantees attached to privacy protection, on the other hand they can led to excessive costs both for public and private institutions.

We're convinced that we do all agree on the need of avoiding harm for economical growth and innovation. Therefore, a balanced and reasonable approach is paramount for dealing with this issue.
The presidency has requested delegations to fill a questionnaire in order to assess the general tendencies on this matter.

The questionnaire covers articles 11, 12, 14, 15, 22, 28, 31, 32. With no doubt these are bureaucratic provisions and there is nothing to say about their inclusion. But the question is if there are other administrative burdens in the draft regulation that should be taken on board as well.
According to our point of view the answer should be affirmative. Articles, 20, 23, 33, 34, 35 to 37, Chapter V, VI and VII, should be considered in the questionnaire.

Thus***, our first remark is that the questionnaire as is, cannot bring a clear picture of administrative burdens in the draft regulation. More provisions should be contained in it.***

Our second remark has to do with the questions provided in the questionnaire and the binary answer mode proposed.

Some times it happens that a specific provision could be acceptable but only if we assume that some new wording is needed. In other cases a binary answer cannot cover all the cases for a particular provision. For example, the question "**Is the size of the entity processing the personal data an appropriate criterion for the application of data protection rules in this case?**" can lead to several considerations that do not fit in a Yes/No answer.

Therefore, our second remark suggests a more open and broad debate about every specific provision, in order to have a clear view of how it behaves in different circumstances.

And finally there is a third remark that has to do with the whole debate on administrative burdens.

According to our point of view a questionnaire-based debate brings an excessively poor approach to the subject as it impedes considering alternative solutions based on tools like accountability, certifications policies or self-regulation.

The use of the above-mentioned tools would require a quite complex surgery on the text rather than a simply article-based redrafting.
Thus, the willingness of the delegations on the use of those tools should be explored.

2. General remarks on methodological approach

As it our last friends of the presidency meeting proved, a sound methodology is needed to deal with horizontal issues.

In our opinion, order matters. The approach for public and private sector should be the first area to deal with because of the large effect that outcomes could have in the whole regulation. Second should come administrative burdens, and finally delegated acts.

The idea of dealing with delegated acts as a last step for the horizontal issues discussion has sense, because depending on the solutions applied in the previous discussions, delegated acts could be less and solutions could change as well.
But procedure is not the only point to be taken in account in order to build up a sound methodological approach.

A second point for a consistent methodology is establishing an adequate link with the desired outcomes. According to this, it should be advisable to know the scope of the horizontal issues debate, namely: do we want to stick to the current draft proposal as is, accepting only some minor changes in recitals or articles, or by the contrary we can accept some approach changes that necessarily involves serious reconsideration of specific parts of the text?

Depending on the answer the methodology to be used could change. If we want to stick to the text accepting only some minor changes, the best way to go might be an article-by-article based analysis using the previously agreed toolbox. If it is not the case, and some major overhaul is accepted, a brainstorming about different alternatives and a DAFO analysis on every particular alternative seems to be necessary.

In any case, a new impact analysis would be necessary as well. Different stakeholders have underlined serious concerns on financial impacts concerning this instrument, and no amendments should be accepted without being sure that those concerns are properly addressed.

We're well aware that those proposals do have a clear impact on workload, but we're also convinced that it is always worthwhile investing time and energy when fundamental rights, growth and innovation, are at stakes.

FRANCE

I. Annex I – Table on the reduction of administrative burdens

The French delegation considers that the draft Regulation should not make any differentiation in terms of the rights of data subjects. But it advocates differentiation of the draft Regulation's provisions, from Chapter IV onwards, in accordance with the criterion of "risks" posed by data processing.

Considering this to be a key criterion, France believes it should inform the whole text. The draft Regulation should therefore define this criterion and make it an essential part of the text. In this connection, removing prior declarations is also likely to be counter-productive when determining the risks posed by the processing of personal data.

For the same reason, the French delegation considers that the other criteria proposed by the table in Annex I to 12918/1/12 REV 1 are not relevant and that it is unnecessary to go into such detail at this stage.

IRELAND

We thank the Cypriot Presidency for this opportunity to contribute on the subject of administrative burdens.

The questionnaire draws a distinction between administrative burdens (i.e. broadly-defined obligations to provide information) and compliance costs, including the additional compliance costs necessitated by the Regulation. This distinction is likely to be seen as somewhat theoretical and artificial from the perspective of data controllers who will be required to undertake additional duties, and bear the associated costs, of demonstrating "for each processing operation the compliance with the provisions of this Regulation" (article 5(f)). The following issues need to be addressed therefore.

Firstly, it will be important to ensure clarity regarding the material scope of the Regulation (including the scope of exemptions referred to in article 2.2) and the definition of 'personal data' in article 4. Secondly, clarity is required in relation to the balancing of data protection rights with other fundamental rights (for example, should the scope of article 80 be extended beyond "journalistic purposes" to include the broader concept "freedom of expression and information" as suggested by the FRA?).

Generally speaking, administrative burdens should be proportionate to the risk of misuse of personal data. It will be necessary, therefore, to reduce, clarify and simplify the obligations on controllers where the risk of misuse is low, while maintaining appropriate safeguards where the risks are real and potentially detrimental to data subjects. Such a risk-based approach is also relevant to the notification of data breaches, data protection impact assessments and transfers of personal data to third countries and international organisations (especially in cases where prior authorisation is foreseen under article 42.2(d)).

In determining risk levels, account could be taken of factors such as: the number of data subjects likely to be affected; the risk of financial loss; the risk of identity theft; whether the data fall into special categories (article 9).

The imposition of additional compliance requirements, and associated costs, also needs to be examined carefully. Such examination is required in the context of article 18 (Right to data portability); article 23 (Data protection by design and default); article 33 (Data protection impact assessment); article 34 (Prior authorisation and prior consultation); article 35 (Designation of data protection officer). In these cases, the accountability principle has an important role to play. In particular, incentives should be provided for controllers (and processors) to adopt 'best practice' models set out in Codes of Conduct (article 38) or certification mechanisms and data protection seals and marks (article 39).

LUXEMBOURG

These comments are without prejudice to any further positioning.

Luxembourg considers that administrative burden generally arises from an overly prescriptive and rigid legislative text. The right balance should therefore be found between an accountability-based approach and a future-proof regulation on the one hand, and legal certainty and clear common rules on the other hand. Indeed, one of the main burdens for controllers active across the single market which resulted from the 1995/46/EC directive is the diverging rules and the ensuing legal fragmentation.

Luxembourg considers that derogations provided for SMEs are too arbitrary as a sole criterion and should be further framed. SMEs whose core business relates to processing data, or that are involved in risky data processing activities, should not be exempted. By the same token, large businesses where data processing may be ancillary to their main activities should not be required to fulfil all obligations. Therefore, the nature of the processing activities should be taken more into account: for less risky data processing, the administrative burden should be lowered. Proportionality should be the guiding principle here, as increased administrative obligations upon controllers may not necessarily result in an increased level of protection of personal data.

Furthermore, administrative burden should not be looked at exclusively. There are also compliance costs that arise from several proposed provisions (eg. DPO, large definition of personal data) and impact controllers. The risk is that the regulation will be difficult to comply with and, at worst, act as a disincentive to innovation and economic growth.

THE NETHERLANDS

The abolishment of the notification requirement of Directive 95/46/EC is one of the most important positive points of the proposal for a General Data Protection Regulation. The various aspects oaf the principle of accountability is, when properly applied, an adequate way to protect data subjects interests and to enhance the level of data protection awareness in public institutions and businesses.

The application of the principle of accountability itself should, however, not lead to greater administrative burdens and compliance costs than the administrative burdens and compliance costs caused by the current notification requirement. Instead efforts should be made to reduce these burdens and costs. This should be done by tailoring burdens and costs according to the level of the risks associated with the processing. The size of the enterprise is not a decisive indicator of the level of risk.
A high level of administrative burdens and compliance costs will affect the acceptance of data protection legislation negatively.

The Regulation requires all data controllers, and to a lesser extent processors, indiscriminately, to provide for transparent information and communication, procedures and mechanisms for exercising data subjects rights, to provide for detailed information and the right of access. The responsibility of the controller to collect and administer a great amount of detailed documentation and to provide for several categories of information in any data breach notification, without any form of distinction as regards the severity of the breach is only partially mitigated by provisions allowing for more tailored requirements for micro, small and medium businesses.

Data Protection Impact Assessment

Proper application of the principle of accountability involves a prior risk assessment. A risk assessment can be made by way of a data protection impact assessment. As the case may be a data protection impact assessment can be preceded by a less formal quick scan in order to assess whether the processing operations constitute a degree of risk that justifies the execution of a formal and full-fledged data protection impact assessment.

The risks that should be assessed are listed in Article 33, para 2 of the Regulation. Some risks can be added, such as the risk of identity theft, the risk of substantive financial loss or damage and the risk of disclosure of data protected by professional secrets and associated privileged communications.

The results of a data protection impact assessment should be decisive when establishing

- the extent of the duty to inform data subjects (notably Art. 14, para 1 (h), of the Regulation)
- the extent of the documentation requirements,
- the extent of the technical and organisational measures to ensure a sufficient level of data security,
- the necessity and in affirmative cases the scale of the duty to notify the supervisory authority and data subject in cases of data breaches,
- the requirement of prior authorisation by or consultation of the supervisory authority
- the necessity to designate a data protection officer

A higher risk justifies higher administrative burdens and specified compliance requirements.

SLOVENIA

I. The Republic of Slovenia expresses at first its general remarks with respect to horizontal issues of administrative burdens concerning the Draft General Data Protection Regulation, as are proposed to be discussed by the Cyprus Presidency. We also welcome this possibility for continuing the systemic and expert dialogue on the Draft General Data Protection Regulation.

II. We opine that the Draft General Data Protection Regulation might resemble in some aspects to a combination of a directive, to which some modernistic aspects have been added, but not finally developed in their details, which is problematic from the viewpoints of legal certainty and legal clarity, which is also related to Slovenia's positions expressed with respect to delegated and implementing acts.

III. While assessing the possible impact(s) of administrative burdens we opine that the existing impact assessment might be a bit unclear with respect to the benefits for business operations, since unclear provisions and also legal lacunae with respect to delegated and implementing acts are not taken into account, which might definitely produce unclear, but in any case highly burdensome activities and related high costs for data controllers, especially those from the private, but also from the public sector. From this viewpoint we especially have to mention the possible costs for performing data protection impact assessments, fines for administrative sanctions and request for instituting data protection officers. The new additional administrative burdens, combined with issue of legal non-clarity might also require very expensive and sometimes even everyday legal (and maybe also technical) advice to be provided, which might be acceptable (partially and only in a self-regulating mode) for big data controllers in private sector, but not for ordinary (every day) data controllers, especially SMEs, it might even put them into competitive disadvantage, might stifle innovation and economic growth - without sufficient or clear added value for the realisation and protection of data privacy as a human (fundamental; individual) right.

IV. From the systemic viewpoint and taking into account the right to data privacy as a human right we opine that the system of regulation under this draft legal act should be streamlined in such a manner that it shall be easily applicable for all types of data controllers, irrespective (mostly) if they are a part of the private or public sector and regulation in this draft legal act should not cause possible years of "wrangling" over its implementation.

V. So, in accordance with our previous positions we express again that the best solution would be to change this legal act into the directive, albeit a directive that should be very detailed, and which would not produce unnecessary but from our viewpoint - predictable "shocks" in its implementation.

VI. The Republic of Slovenia also reserves for the future process of experts` dialogue at the DAPIX the possibility to add additional comments or reservations and points that issues of existence and solution of problems of administrative burdens have to be discussed always in the setting of each provision or system, to which they are a part of.

VII. Slovenia's systemic and brief positions on non-exhaustive list of provisions with administrative burdens or unclear provisions that might produce administrative burdens are expressed onwards from the next page of this document

SWEDEN

Sweden welcomes the Presidency's initiative to discuss the issue of administrative burdens separately from the article-by-article reading of the proposed Regulation. We are concerned about the new administrative burdens and requirements in the proposal and remain convinced that this issue requires a horizontal approach.

Initially we would like to underline that the discussion should cover a ***wider range of articles*** than those set out in the questionnaire, such as the obligation to appoint a data protection officer, the right to data portability, data protection by design and data protection by default.

The burdens placed on controllers need to be thoroughly assessed and, as indicated in the Presidency´s paper, pass a test of proportionality. New administrative burdens should only be introduced if they are ***proportionate in relation to the benefit*** for the protection of individuals' privacy.

In order to achieve proportionality there is a need for ***a risk and context based approach***. The proposed Regulation has a very wide scope, ranging from commonplace processing (e.g. the use of e-mail programs, Skype and social media) to high-risk processing (e.g. profiling and health care databases). If data protection rules are modelled to mitigate the dangers of high-risk processing, unnecessary obstacles for commonplace processing may be created. On the other hand, if data protection rules are adapted to commonplace processing they may prove too lenient for high-risk processing. Hence, there is a need for a differentiation of the rules based on the risks involved and the context of the processing.

In our view, ***a risk and context based approach should ideally be implemented in a horizontal manner***, meaning that the proposal should be amended in a more comprehensive way than merely adjusting the different articles. The criteria by which to determine whether processing is risky could for instance be defined in a separate article in the Regulation. It also follows from the above mentioned that it is not possible to answer the question of proportionality in the Presidency´s paper by simply stating Yes or No for each article.

The ***size of the controller*** may often be an adequate factor to take into account. However, in many cases there is a need to take into account other factors as well. Processing carried out by small or medium size controllers may have considerable variation and, thus, require different safeguards. For instance, for a small restaurant which only processes personal data for the sake of keeping track of reservations, the obligation to adopt a data protection policy seems to onerous, while this obligation might be completely reasonable for an equally small company that deals with massive amounts of personal data or profiling. Further, it should be borne in mind that the same controller may engage in both high risk and low risk processing. A medical research company may for example process highly sensitive genetic data, on the one hand, and carry out low-risk processing (e-mail and IP telephony) for internal administration and communication, on the other.

The limited exemption for household use means that the rules of the Regulation may often apply to ***processing performed by natural persons as part of their daily life***. For example, it follows from the wording of the Regulation that a person posting any personal data (e.g. names) on his public social network page is in principle subject to the obligation to adopt a data protection policy. However, it is obvious that this and many of the other obligations in the Regulation cannot in practice be applied to such processing. We believe that processing carried out by natural persons need to be exempted from a number of the provisions in the Regulation, e.g. the obligation to have a data protection policy and the provisions on data protection by design and default

UNITED KINGDOM

The United Kingdom welcomes this opportunity to respond on the horizontal issue of Administrative Burdens in respect of the proposal for a General Data Protection Regulation and we are grateful to the Cyprus Presidency and the Council Secretariat for devising and facilitating this process. The UK also welcomes the forthcoming opportunity to comment in a similar way on the application of data protection rules to the public sector.

The UK questions the Commission's narrow definition of "information requirements" when considering the impact of administrative burdens. With this in mind, it is the UK view that the EU Commission impact assessment over-estimates the benefit to business as it does not take account of a number of measures that will have ongoing costs. The figure cited by the Commission of a reduction in administrative burdens for business of a magnitude of €2.3 billion per annum, does not take account of other costs to business, such as employing data protection officers, the costs of carrying out data protection impact assessments and the cost of dealing with additional subject access requests (Article 12) that will arise from the removal of the fee. It is also the UK view that the cost of notifying data protection breaches to the supervisory authority is likely to be higher than €20 million quoted, as the Commission estimates only an additional 1,000 data breaches will be notified to supervisory authorities when a recent survey suggests that the true figure is likely to be considerably higher.[1]

We would also contend that the level of administrative burden presents a particular challenge for SMEs, since they will not have the ability to absorb any extra costs in the same way that large corporations might be able to. There are three examples of qualified exemptions written into the text for Small and Medium Enterprises of fewer than 250 employees. These are in regards to obligations around data protection officers; the keeping of documentation; and the new fines regime. While we support the principle of exemptions for SMEs, we want to see a proportionate data protection framework for all businesses, SMEs included, which takes into account risks of processing, sensitivity of data and number of data subjects. We believe that this is the most effective way to go about protecting SMEs and businesses in general from undue administrative burdens.

[1] PWC (2012), 'Information security breaches survey: technical report'.

In addition, tougher sanctions, including the possibility of fines of up to 2% of a company's global annual turnover for breach of requirements in the proposed Regulation, are likely to further compound the level of administrative burdens faced by organisations as they are likely to take an overly cautious approach to data protection measures that is disproportionate to any gains achieved.

In particular, the UK would make the case that:

- The requirement to notify breaches within 24 hours should be dropped, and the notification requirement restricted to serious breaches which takes account of the amount of personal data that is processed and the sensitivity of that data while at the same time ensuring consistency with breach notification requirements set out in the e-privacy Directive.

- The requirement for all processing activity to be documented is overly prescriptive. The sheer amount of information to be documented makes this requirement onerous for organisations to comply with and we would question whether the requirement for policies and administrative measures to demonstrate compliance with the draft regulation will lead to effective accountability

- support a system of administrative penalties for serious breaches of the Regulation's requirements, but push for a more proportionate level of maximum fines, which allows supervisory authorities greater discretion in applying the powers available to them; we are concerned, for example, that a Supervisory Authority will be required to take action against a controller whose processing is fair and lawful, and does not negatively impact on an individual's privacy, merely because the controller does not have the necessary documentation in order or is non- compliant with one of the other buraucratic process requirements of the Regulation.

- The use of delegating acts to prescribe electronic formats for information to the data subject could add to the burdens on data controllers.

In conclusion, our overarching objective is to create a data protection framework that works for all sectors and organisation types, and supports the rapidly growing digital economy sector in the UK. Although a proportionate and sensible data protection system can help economic growth, an unwieldy and burdensome regime can have the opposite effect. Therefore, we would also welcome further consideration of a co-regulatory approach where this is appropriate.

_____

ARTICLE OF DRAFT DP REGULATION	PROPORTIONALITY PRINCIPLE	CRITERIA PROPOSED IN DRAFT DP REGULATION (not mutually exclusive)		OTHER/ADDITIONAL POSSIBLE CRITERIA (not mutually exclusive)			
	Proportionality Test – is the obligation proportional, particularly in terms of the burden it imposes on micro, small, and medium-sized enterprises as compared to large enterprises? (YES/NO)	**Is the size of the entity processing the personal data an appropriate criterion for the application of data protection rules in this case? (YES/NO)**	**Risk involved in the processing activities (e.g. sensitivity of data, systematic monitoring of data subjects) (YES/NO)**	**Volume of personal data processed (YES/NO)**	**Number of data subjects affected (YES/NO)**	**Which category of data subjects is affected (e.g. minors) (YES/NO)**	**Other (please specify)**
Article 11 Transparent information and communication **1.** The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data	**YES**: BE, BG (The text of the provision provides for free choice of data controllers with regard to the means and methods of performing this obligation, as well as, to the form and content of the envisaged accessible policies), CZ (for large), IT (This is a general obligation irrespective of size: it	**YES**: CZ (But not exclusive (reality check – off line world problematic, on line world uses this for gaining customers' trust even if it is not yet obligatory), LU (But only if articulated with other criteria such as the risk of the processing)	**YES**: DE, ES (assuming some redrafting), IE, IT, PT, NO, SE, RO, EE, DK, LU	**YES**: BG (Only with regard to the particular means and methods for fulfilment of this obligation), EE, ES (assuming some redrafting), IE, LT, EE	**YES**: BG (Only with regard to the particular means and methods for fulfilment of this obligation), EE; ES (assuming some redrafting), IE, LT	**YES**: BG (Only with regard to the particular means and methods for fulfilment of this obligation), EE, ES (assuming some redrafting), LT, RO	DE (See general remarks)[1] ES (ACCOU-NTABILITY BASED APPROACH) **NO**: HU DK, SE (See general remarks)

[1] DE: Article 11, like Articles 12 and 22, contains overarching and/or advance transparency obligations and/or procedural requirements for data processors, which must be considered in the overall context of the obligations specifically imposed by Article 14 et seq. and Article 23 et seq. Here, unnecessary red tape can be stripped down to the essentials by streamlining rules and reducing specifications.

subjects' rights.	may not be made conditional on the entity processing data), LT (The enterprises should have policies with regard to the processing of personal data and for the exercise of data subjects' rights and this obligation could be determined by the categories of processed data and the purposes of the processing. The requirement to adapt information to every data subject will require disproportionate efforts by controllers so distinction can be made only between adults and children, as a data subjects), HU, PT, FI, RO, MT, LU **NO**: CZ (for small), DE, ES, EE, IE, NO, SE (There are no exemptions in this article or article 22 from the obligation to adopt a policy for e.g. low-risk processing by SMEs or even natural persons. The requirement to adapt information to the data subject could be burdensome for small	**NO**: BG (Not in this case. The provision is flexible enough which allows for all data controllers to successfully fulfil this obligation notwithstanding their size and the legal form of the entity), DE, ES, FR, IE, IT, LT, HU, PT, NO, FI, RO, EE, MT DK, SE (See general remarks)	**NO**: BG (Insofar this obligation refers to the provision of general information concerning the implemented data protection policy, and does not foresee granting of public access to personal data), CZ, FR, LT, HU, FI, MT	**NO**: CZ, FR, HU, PT, FI, RO, MT DE (See general remarks) DK, SE (See general remarks)	CZ (Maybe, but practice would sort it out as an issue of competition) DE (See general remarks) **NO**: FR, HU, PT, FI, RO, MT DK, SE (See general remarks)	**NO**: CZ, FR, HU, PT, FI, MT DE (See general remarks) DK, SE (See general remarks)	UK (There are no criteria set out in the Regulation for this article. However, it would be helpful to relax the level of prescription here, particularly for SMEs processing non-sensitive data) SI (There is a general loophole with respect to criteria for this activity of data controllers, which is not problematic just form the viewpoint of data privacy as a human right, but also from the viewpoints of legal certainty and clarity, as well as costs planning. And everyday (small risk) processing operations should not be covered. In general - it

	controllers), UK (This article will have costs to controllers due to the requirement to ensure that processing is 'transparent'. The Commission estimate there will be a one-off cost to controllers of €100 through providing intelligible information to data subjects. However, we would expect this to be an ongoing cost that will be particularly burdensome to SMEs. The requirement to adapt the format to the data subject is likely to be particularly burdensome for small controllers), FI[1], DK (There are no exemptions in this article or article 22 from the obligation to adopt a policy for e.g. low-risk processing by SMEs or even natural persons. The requirement to adapt information to the data subject could be burdensome for small controller), SI NL (Para 1 is difficult							would be very advisable to establish a favorable criterion of "ordinary processing" of personal data (every-day business operations that are performed "on average" by every data controllers) - taking into account that this should not include processing of sensitive personal data or risky processing of personal data. Therefore, it is hard to propose any achievable solutions)

[1] […] indicates that a certain part of the text has been omitted, namely provisions concerning delegated and implementing acts as these are dealt with in separate tables.

	to assess in terms of proportionality, due to the yet unclear meaning of "policies". Para 2 No)						
2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.	**YES**: BE, NO, MT **NO**: EE, IE, FI (As regards the requirements relating to the intelligible form, clear and plain language etc. the obligation seems proportional. However, the obligation to provide information and communication should be limited to the requirements laid down in the Regulation. The current formulation "*any* information and *any* communication *relating* to the processing of personal data" seems to be too broad), LU, SI	**NO**: IE, FI, EE, MT	**NO**: FI, EE, MT **YES**: LU	**NO**: FI, EE, MT	**NO**: FI, EE, MT	**NO**: FI, EE, MT	EE (The obligation for the controller to provide any information and any communication is problematic, because it is not specified, whether the information should be provided upon request or always pre-emptively. Hence, it would be less burdensome to provide certain criteria of information or the information should be provided upon request)
Article 12 Procedures and mechanisms for exercising the rights of the data subject	**YES**: BE, BG (Insofar the data subjects have equal rights that have to be exercised equally, notwithstanding the size of the controller. A contrary interpretation	CZ (YES on (1) NO on (4). While establishing procedures under (1) is easier for large controllers, their size probably would not diminish burden with	**NO**: BG (The provision refers to the establishment of procedures and mechanisms, i.e. it is of technical and organizational nature and does not involve a data	**NO**: BG (The provision refers to the establishment of procedures and mechanisms,	**NO**: BG (The provision refers to the establishment of procedures and	**YES**: BG (Insofar the established procedures should be accessible for all categories	DK, DE, SE (See general remarks) ES (ACCOUNTABILITY BASED

1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.	would mean that for the different controllers (small, medium-sized and large) different regulations shall apply which will unreasonably impede the enforcement of data subjects' rights, as well as the control exercised by data protection authorities. This obligation put emphasis on the end result – providing of information – and allows for more flexibility regarding the mechanisms of its fulfillment by data controllers), CZ (for large on (1)), IE, IT (This is part of the standard obligation under the current directive and leaves room for data controller to devise the appropriate mechanisms), HU, NL, PT, NO, RO, MT, LU **NO**: CZ (for small on (1) and (4), on (4)), EE, ES, LT (The procedures and mechanisms for exercising the rights of the data subject should be regulated in the Regulation and extra	papering over excessive requests (4), as that is more dependent on number of data subjects and on visibility of controller) **YES**: LU **NO**: DE, EE, FR, IE, IT, LT, HU, NL (No. The size of the entity processing the personal data is not an appropriate criterion for the application of data protection rules. This should be replaced by a risk assessment in the form of a data protection impact assessment which must indicate what safeguards and duties of the controller (or as the case may be the processor) should mitigate the risks involved. A higher risks justifies a havier burden on the controller or processor in terms of specific duties and obligations. A lower risks justifies a lighter burden in terms of specific duties and obligations. A very low risk justifies the application of the	processing risk), ES, EE, FR, LT, HU, FI, MT **MAYBE**: CZ **YES**: DE, IT, NL, PT, NO, SE, RO, DK, LU	i.e. it is of technical and organizational nature and does not involve a data processing risk), CZ, ES, FR, LT, HU, PT, FI, RO, MT DK, DE, SE (See general remarks) **YES**: IT, NL	mechanisms, i.e. it is of technical and organizationa l nature and does not involve a data processing risk), ES, EE, FR, LT, HU, PT, FI, RO, MT **MAYBE**: CZ DK, DE, SE (See general remarks) **YES**: IT, NL	of data subjects), IT, NL, RO **NO**: CZ, ES, EE, FR, LT, HU, PT, FI, MT DK, DE SE (See general remarks)	APPROACH) EE (We suggest covering this issue by self-regulation) **NO**: HU UK (The Regulation states that "appropriate measures" for micros and SMEs shall be taken when specifying the electronic format in which information must be given. More detail on what this means in practice is needed. However, we advocate more flexibility in this article for all data controllers by allowing a fee to be charged for responding to a request for information, and not specifying electronic

	obligation to establish procedures for providing the information and for the exercise of the rights of data subjects for each controller is not necessary and imposes disproportionate burdens. The controller's right to charge a fee for providing the information to the data subject (the paragraph 4 of the Article 12) is questionable, since the controller may set unreasonably high fee and complicate the implementation of the rights of the data subject. Instead of proposed regulation could be considered the scheme then the data controller shall provide the information to the data subject free of charge once per calendar year. When such data are disclosed for a fee, the amount of the fee may not exceed the cost of disclosure of the data (preparations of information requested, copies of documents requested and etc.), SE	normal duty to weigh or balance the interests of the controller and the data subject, supported by a normal level of enforcement, but without specific duties. No risk might justify exclusion or exemption from certain rules of the Regulation), PT, NO, FI, RO, MT ES (not necessarily) DK, SE (See general remarks) SI (The size of data controller should not be a guiding principle at all. The issue of risky data or risky processing should be guide to solving this issue. Also, it is doubtful, whether the proposed legal act is really technologically neutral)					formats in which data must be held. There also needs to be clarification on what is meant by 'manifestly excessive' requests)

	(The rules regarding the time limits to provide information as well as the obligation to provide information in an electronic form are too inflexible. The exemption for manifestly excessive requests seems insufficient), UK (This removal of the fee will lead to a rise in UK Subject Access Requests (SARs) which will be an additional burden on business. The UK estimate that the number of SARs could increase by 25-40 per cent, which is a cost of £12-£37 million (€15-€46m) for UK businesses with over 80% of this cost going to SMEs. The requirement to provide the data in a specified electronic format is also likely to have additional costs, as is reducing the time limit for a response from 40 days to one month), FI[1] (This paragraph does not seem to be proportional. It does not seem necessary to lay down						

[1] […] indicates that a certain part of the text has been omitted, namely provisions concerning delegated and implementing acts as these are dealt with in separate tables.

	particular mechanisms for facilitating the request for the action here. Instead, it is essential that every operator conduct their duties. The requirement to provide electronic means for requests in certain cases appears proportional), DK (The rules regarding the time limits to provide information as well as the obligation to provide information in an electronic form are too inflexible. The exemption for manifestly excessive requests seems insufficient), SI						
2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data	**NO**: BE, IE, EE, NO (We agree that the information shall be given in writing, but we believe it should be left to the controller to decide the manner in which the information shall be provided), MT **YES**: FI (The matter regulated in this paragraph is of high importance. It needs to examined and assessed in more detail. At this stage, red together with Article 13 and 15-19	**NO**: IE, EE, MT FI (Might be relevant)	FI (Might be relevant) **YES:** EE, MT	**YES**: FI, EE, MT	**YES**: FI, EE **NO**: MT	**YES**: EE **NO**: MT FI (May be not)	BE (Considers that the period of one month is too short. BE would like to change in 2 months) EE (The written form of the answer to the request of the data subject is problematic)

subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.	this paragraph raises some questions. Size of entity; Might be relevant, such factors as field of activity could be taken into consideration. Risk involved in the processing; Might be relevant) MT (*Request by one data subject may also involve a disproportionate effort. The prolongation for a further month should therefore also apply in such cases)*						

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.	**YES**: BE, IE, FI[1] (This seems proportional. However, the final assessment is connected to the content of some other Articles), MT, LU **NO**: NO (We agree that the controller should inform the data subject of the reasons for the refusal, but we are in doubt as to whether it is reasonable to require that the controller gives information on the possibility of lodging a complaint to the supervisory authority, and particularly on the possibilities of seeking judicial remedy, in all cases)	**NO:** MT	**NO:** MT	**NO:** MT	**NO:** MT		
4. The information and the actions taken on requests referred to in paragraph 1 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	**NO**: BE, IE **YES**: NO, FI[6] (Not to charge anything when providing the information and taking action seems proportional. However, this paragraph has caused some questions), MT, LU	**NO:** MT	**NO:** MT	**YES**: MT	**YES**: MT		BE (The criteria for assessing whether a request is « *manifestly excessive*» are not clear. BE asks COM to specify those criteria in a recital)

[1] […] indicates that a certain part of the text has been omitted, namely provisions concerning delegated and implementing acts as these are dealt with in separate tables.

information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.[1]							
Article 14 Information to the data subject **1.** Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:	**YES**: BE, IT (with some exceptions (however, not relating specifically to the fact that the DC is a SME) Paragraph 1c: it may be impossible for the DC to provide this information at the time of data collection, there is anyhow the general requirement of not storing data for any longer than necessary for the specific purposes, which must be specified under 1b). Paragraph 1f: to consider whether "categories" of recipients is more appropriate (impossibility of providing information on all individual	**YES**: BG CZ (Partially Large controllers may bear the burden easier) **NO**: DE, EE, ES, FR, IE, IT (Again, this would go against general transparency obligation that may not be conditional upon size), LT, HU, NL (The size of the entity processing the personal data is not an appropriate criterion for the application of data protection rules), PT, NO, RO, MT, LU DK, SE (See general remarks) SI (We opine that it is problematic that there are	**NO**: BG, CZ, FR, HU, RO, MT **YES**: DE, EE, ES (in same cases), IE, IT, LT, NL, PT, NO, SE, DK, LU	**NO**: BG, EE, ES, FR, LT, HU, PT, RO, MT **MAYBE**: CZ DE (See general remarks) **YES**: IE, IT (might be taken into account to define the "disproportion ate effort"), NL, LU DK, SE (See general remarks)	**NO**: BG, EE, ES, FR, LT, HU, PT, RO, MT **MAYBE**: CZ DE (See general remarks) **YES**: IE, IT (To define disproportion ate effort), NL, RO DK, SE (See general remarks)	**NO**: BG, CZ, EE, FR, HU, PT, MT **YES**: ES, IE, LT, NL DK, SE (See general remarks) UK (The Regulation states that different criteria can be set out for certain sectors and SMEs. This seems correct in principle, but without knowing what this	BG (The activities performed by the controller and the type of the data processed relating to these activities) DK, DE (See general remarks) EE (The list of the data is too elaborate. The data should be provided upon request, not pre-emptively. The stipulation should be further discussed, to find reasonable

[*] […] indicates that a certain part of the text has been omitted, namely provisions concerning delegated and implementing acts as these are dealt with in separate tables.

	recipients). Paragraph 1h: too broad ranging, better to specify at least some items of additional information that must be in any case provided (PIA, profiling, etc.), HU, PT, RO, MT, LU (Except (c)) **NO**: BG (Insofar that small enterprises are not expected to appoint data protection officer, who could facilitate the communication between the controller and data subjects), DE, ES, EE, IE, LT (It is not clear if data subject should be provided with all the information specified in the Article 14 Paragraphs 1 and 2 in all cases not regarding what the coverage of data subject's request is. Such regulation would cause significant administrative and partially financial burden because the scope of information is fairly broad), NL, SE (The obligation to provide all the specified information is not proportionate for, inter	no criteria provided, again)				criteria is, it is difficult to determine whether it is proportional)	balance) ES (ACCOUNTABILITY BASED APPROACH) **NO**: HU **NL** (Risks can be specified according to underlying principles or values, such as: • risks mentioned in article 33, para 2 • risk of ID theft when data are disclosed • significant damage to personality, moral standing etc. • significant financial damage breach of confidence which is protected by privileged communications (such as physicians, lawyers etc) SE (See general remarks)

	alia, low risk processing by SME:s or natural persons. The exemptions are insufficient. It is not always known how long the data will need to be stored), UK (This obligation is not proportional due to the nature of the information that the individual must be provided with. Article 14 expands the information that the data subject must be provided with to include the period for which the data will be stored and the recipients of personal data, with further prescription allowed for in a delegated act. If it is not possible to provide this information in a generic privacy notice then this will be costly for data controllers), DK (The obligation to provide all the specified information is not proportionate for, inter alia, low risk processing by SME:s or natural persons. The exemptions are insufficient), SI						UK (It is not possible for data controllers to specify how long the data will be stored and so this should be removed for all controllers. The delegated act allowing the Commission to specify criteria should be dropped) SI (It has to be left either to national law or a significant degree of flexibility allowed in this legal act to data controllers (in a general form, but within a certain framework) to establish data retention periods, which should of course also be transparent. The issue of further processing of personal data

	CZ (Sometimes for small. Depends on setting (online, other) (1) is too extensive (2) goes too far. Sometimes for large. Depends on setting (online, other) (1) is too extensive (2) goes too far						and its compatibility should also be taken into account)
(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;	**YES**: BE, NO, FI[1], MT	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	
(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);	**YES**: BE, FI[8] **NO**: NO (We feel that it is unnecessary to include the terms and general conditions under article 6 nr.1 b), MT MT (*Including the contract terms and general conditions when explaining processing operations is excessive and cumbersome)*	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	

[1] […] indicates that a certain part of the text has been omitted, namely provisions concerning delegated and implementing acts as these are dealt with in separate tables.

(c) the period for which the personal data will be stored;	**NO**: BE, NO (The wording should be made more flexible), MT **YES**: FI MT (*It is difficult to clear the retention period every time with National Archivist)*	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	BE (Considers that it is not always possible to determine the retention period of the data. BE wants to complete point (c) and article 15.1 d) with "where known")
(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;	**YES**: BE, NO, FI, MT	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	
(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;	**YES**: BE, FI, MT **NO**: NO (in doubt as to whether it is reasonable to require that the controller gives information on the possibility of lodging a complaint to the DPA and the contact details of the authority in all cases)	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	
(f) the recipients or categories of recipients of the personal data;	**NO**: BE **YES**: NO, FI, MT	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**BE ((f)** ~~the recipients or~~ The categories of recipients of

							the personal data;)
(g) 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;	**YES**: BE, MT **NO**: NO (We agree that information on the intention of transferring the data should be given, but we do not think it is proportional to give information on the level of protection offered in all cases)	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	
(h) 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.	**NO**: BE **YES**: NO, FI, MT	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	BE (Considers that the wording of paragraph (h) is too broad. BE asks COM to clarify the scope of this paragraph)
2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of	**YES**: BE, EE, NO, FI, RO, MT, LU	**NO**: FI, RO, MT	**NO**: FI, RO, MT	**NO**: FI, RO, MT	**NO**: FI, RO, MT	**NO**: FI, RO, MT	EE (The wording of the stipulation should be revised. The obligation to distinguish obligatory and voluntary data is proportional, but the

personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.							obligation to inform about obligatory data is questionable. We suggest binding the obligation to inform with situation, where data collected is processed for different purposes)
3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.	**NO**: BE, LU (is this information to be provided on request from the data subject?) **YES**: NO, FI, RO, MT	**NO**: FI, RO, MT **YES**: LU	**NO**: FI, RO, MT **YES**: LU	**NO**: FI, RO, MT	**NO**: FI, RO **YES**: MT	**NO**: FI, RO, MT	BE (Considers that it is impossible to inform the data subject of the entire source and proposes to add the wording "categories of") MT (*Yes if data is public domain)*
4. The controller shall provide the information referred to in paragraphs 1, 2 and 3: **(a)** at the time when the personal data are obtained from the data subject; or	**YES**: BE, NO, FI (The administrative burden caused by this paragraph seems proportional. However, the paragraph itself remains rather unclear), RO, MT, LU	**NO**: FI, RO, RO, MT	**NO**: FI, RO, MT	**NO**: FI, RO, MT	**NO**: FI, RO, MT	**NO**: FI, RO, MT	
(b) where the personal data are not collected from the data subject,	**YES**: NO	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	

at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.							
5. Paragraphs 1 to 4 shall not apply, where: **(a)** the data subject has already the information referred to in paragraphs 1, 2 and 3; or	**YES**: BE, NO, FI, RO, MT, LU	**NO**: FI, RO, MT	**NO**: FI, RO, MT	**NO**: FI, MT **YES**: RO	**NO**: FI, MT **YES**: RO	**NO**: FI, MT **YES**: RO	RO (Other criterion: - Purpose of the processing - data quality)
(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or	**NO**: BE **YES**: NO, FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	BE (5.1.(b) The data are not collected from the data subject and the provision of such information proves impossible, ***impractical, ~~or~~*** would involve a disproportionate effort ***or would impair other legitimate***

							interests of the controller or vital interests of the data subject; or)
(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or	**YES**: NO, FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	
(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.	**YES**: NO, FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	**NO**: FI	
6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.	**YES**: BE, NO (However we doubt the necessity of this provision), RO, MT **NO**: EE, LU FI (Commenting this paragraph at this stage does not seem possible as the paragraph seems rather unclear and broad. (For example appropriate measures and legitimate interest?)	**NO**: EE, RO, MT	**NO**: EE, RO, MT	**YES**: EE, RO **NO**: FI	**YES**: EE, RO **NO**: FI	**YES**: EE, RO **NO**: FI	

Article 15 **Right of access for the data subject** **1.** The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:	**NO**: BE, CZ (For small. Due to extent of (1)(b), (d) and (h) and to modalities in 12(4). For large. Due to extent of (1)(b), (d) and (h) and to modalities in 12(4)), DE, EE, NL, SE (The right to obtain confirmation at any time could prove dis-proportionate considering that the information must be free of charge. The obligation to provide information in an electronic form is too inflexible. It is not always known how long the data will need to be stored), UK (As with other articles, the specification of certain formats in which data must be provided could be burdensome for businesses, particularly SMEs. It may also not be possible for the controller to set out how long the data will be held for), DK (The right to obtain confirmation at any time is disproportionate considering that the information must be free of charge), SI **YES**: BG (As far as data subjects shall have equal rights that have to be equally enforced before all data controller), ES (assuming that some	**YES**: BG (In view of the fulfillment of this obligation by data controllers – big controllers shall appoint DPO's to facilitate them to comply with this obligation) **PARTIALLY**: CZ (Larger entities may bear the burden more easily) **NO**: DE, EE, ES, FR, IE, IT, LT, HU, NL (The size of the entity processing the personal data is not an appropriate criterion for the application of data protection rules), PT, NO, RO, MT DK, SE (See general remarks) UK (There are no criteria set out in the Regulation, but easing the burden on small controllers would be sensible in the ways suggested for articles 12 and 14) SI (We opine that it is problematic that there are no criteria provided, again)	**YES**: BG (The risk is relevant, as far as the data controller shall undertake appropriate measures for granting access only to the data subject to whom the personal data refer), EE, NL, PT, NO, SE, DK **NO**: CZ, DE, ES, FR, IE, IT, LT, HU, RO, MT	**YES**: BG, NL, PT **NO**: CZ, DE, EE, FR, IE, LT, HU, RO, MT ES (It's basic right) DK, SE (See general remarks)	**YES**: BG, LT, NL, PT **NO**: CZ, DE, EE, FR, IE, LT, HU, RO, MT ES (It's basic right) DK, SE (See general remarks)	**NO**: BG, CZ, DE, EE, FR, IE, HU, RO, MT ES (It's basic right) **YES**: NL, PT DK, SE (See general remarks)	BE (Considers that "at any time" is too broad. 15.1. The data subject shall have the right to obtain from the controller ~~at any time~~, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed ***and*** the controller ***can reply to this request without gathering additional personal data, the controller*** shall provide the following information) CZ (Frequency, shared costs, simple rules) EE(The data should be provided upon request, not pre-emptively) **NO**: HU DK, SE (See general remarks)

	redrafting is necessary), IE (Reasonable intervals), IT (This is, again, a fundamental pillar of data protection and in no way different from the current situation; it is information the data controller already has at its disposal), LT (Although it is important to ensure the data subject's right to access their own personal data, however the right to information should be drafted in such a manner that it would not lead to misuse of the right. The words „at any time" might be deleted, as controllers could may be overwhelmed by frequent requests and some concrete safeguards for misuse of this right shall be introduced in the Regulation), HU, PT, FI[1], RO, MT, LU (In principle. Delete "at any time". Points (g) and (h) should be dependent on other criteria)						UK (As above, provide for flexibility for controllers in the way that information is provided to the data subject and drop the requirement to state how long the data will be held for) SI (There has to be a flexible way provided for the manner how shall the data controllers perform such functions, either by national law, or maybe by guidance of national supervisory bodies, taking into account different sectors, different processing operations, different sensibilities)
(a) the purposes of the processing;	**YES**: BE, NO, FI						

[1] […] indicates that a certain part of the text has been omitted, namely provisions concerning delegated and implementing acts as these are dealt with in separate tables.

(b) the categories of personal data concerned;	**YES**: BE, NO, FI						
(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;	**YES**: BE, NO, FI						
(d) the period for which the personal data will be stored;	**NO**: BE, NO (The provision should be given a more flexible wording). FI						BE (See comment on article 14.1 c))
(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;	**YES**: BE, NO, FI						
(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;	**YES**: BE, FI **NO**: NO (We are in doubt as to whether it is reasonable to require that the controller gives information on the possibility of lodging a complaint to the supervisory authority and the contact details of the authority, in all						

	cases)						
(g) communication of the personal data undergoing processing and of any available information as to their source;	**NO**: BE **YES**: NO, FI						BE (Notes that paragraphs 15.1 g) and 15.2 are the same. What is the link between the two?) The wording of article 15.1 g) is too broad.
(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.	**NO**: BE **NO**: NO (The provision in litra h should be given a more flexible wording) FI (Commenting this paragraph at this stage does not seem possible as the paragraph seems rather unclear and broad. (For example appropriate measures and legitimate interest?))						BE (15.1.h the significance and envisaged consequences of such processing***~~, at least in the case of measures referred to in Article 20~~)***
2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise	**YES**: BE, NO (First sentence), FI, MT, LU **NO**: NO (Last sentence: We believe it should be left to the controller to decide the manner in which the information shall be provided)	**NO**: MT **YES**: LU	**NO**: MT	**NO**: MT	**NO**: MT	**NO**: MT	BE (15.2. bis (new) ***The right of access shall exclude any information whose disclosure could prejudice the securing, protecting and maintaining the resiliency of one or more information systems, for***

requested by the data subject.							***example the algorithms used in the processing)***
Article 22 Responsibility of the controller[1] **1.** 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.	**NO**: BE, BG, CZ (for small as regards policies in (1), otherwise 5(f) is repeated Specific duties in (2) dealt with in relation to relevant Articles), DE, ES, IE, IT (In particular as for keeping the documentation mentioned in Article 28. The rules specify that the data administrator must verify, if necessary by means of internal or external auditors, the effectiveness of the measures implemented to guarantee the lawfulness of the processing for which he is responsible and whether or not it is performed in compliance with the Regulation. The provisions need to be further modified, to ensure that no excessive burden is placed on the data administrator, who is required at all times to assess the suitability of the measures taken to comply with the general requirements, and bears legal liability for any non-	**YES**: BG, CZ (Larger entities may bear the policy paperwork burden more easily), IE, IT, LT **NO**: DE, ES, FR, HU (The sheer size of the data controller seems quite irrelevant with regard to the potential risks stemming from certain data processing activities that might affect the data subjects), NL (The size of the entity processing the personal data is not an appropriate criterion for the application of data protection rules), PT, NO, RO, MT DK, SE (See general remarks)	**YES**: BG (Because it is necessary to perform impact assessments in case of risk processing under Art. 33), DE, FR, IE, IT, LT, HU, NL, PT, NO, SE, DK, LU (linked with impact assessment in article 33) **NO**: CZ, RO, MT ES (In some cases and depending on the accountability approach)	**YES**: BG, IE, IT, HU, NL **POSSIBLY**: CZ (Few data would put in doubt policy paperwork even for large entities) DK, DE SE (See general remarks) **NO**: ES, FR, LT, PT, RO, MT	**YES**: BG, IE, IT, HU, NL **POSSIBLY**: CZ DK, DE, SE (See general remarks) **NO**: ES, FR, LT, PT, RO, MT	**YES**: BG (Because of the requirements with regard to the obligation for maintaining documenta-tion), IT, LT, HU, PT **NO**: CZ, FR, RO, MT DK, DE, SE (See general remarks) ES (In some cases)	BE (Considers that this provision introduces an absolute obligation instead of an obligation of means. BE proposes to turn "*who shall ensure and demonstrate*" into "*who shall be able to demonstrate*") BG (Categories of recipients and possible data transfers) DK, DE, SE (See general remarks) ES (Accountability based approach) IT (Outcome of impact

[1] Article 22 covers also the evidence and documentation the controller shall provide to ensure compliance with other relevant provisions of this Chapter, as referred to in the Article.

	compliance or non-fulfilment. The criteria relating to responsibility should, however, take into account the size of the controlling entity, the nature of the data and the impact of the processing), LT (Since the obligation to store the documentation (Subparagraph a of the Paragraph 2 of the Article 22) requires additional human, technical and financial resources and a real benefit for the data subjects is doubtful, the data controller could keep the documentation on a voluntary basis. The obligations, which are set in the Subparagraphs b-d of the Paragraph 2 of the Article 22, ensure a high level of data protection and should be respected. The obligation to designate a data protection officer (Subparagraph e of the Paragraph 2 of the Article 22) should not be based on the size of the company, but on the amount and categories of the processed data, as well as on the number of the employees who are directly involved in the processing of personal data operations. The obligation to ensure that, if proportionate,							assessment) HU (• the legal basis of data processing (processing based on MS or union law vs. processing based on consent) • the source of personal data (data subject vs. third party) • the type of the processed personal data (sensitive/biometric data vs. non-sensitive/non-biometric data) • the means of data processing (automated vs. manual) UK (There are no criteria set out in the Regulation, other than for documentation where SMEs

	verification of the effectiveness of the measures referred to in paragraphs 1 and 2 of this Article should be carried out by independent internal or external auditors (Paragraph 3 of the Article 22) imposes too high financial burden on SMSs and even large enterprises. **So it might be provided that t**he data controller could recruit independent internal or external auditors on its own initiative and discretion), NL, NO (We are in doubt as to whether this provision is necessary, it could be sufficient that the obligations derive directly from the articles mentioned in paragraph 2 litra a to e), SE (There are no exemptions in this article or article 11 from the obligation to adopt a policy for e.g. low-risk processing by SMEs or even natural persons), UK (The EU Commission Impact Assessment estimated that it would cost each controller €200 every three years to demonstrate compliance with the Regulation. This is intended to cover all of the additional administrative tasks that the controller is expected to carry out and so is a significant under-estimate						whose processing is ancillary to their main activities are exempt. We support an overall reduction in the additional burdens placed on controllers by reducing the documentation that must be kept, and providing further restrictions on what type of processing prior authorisation and consultation with the supervisory authority is needed) SI (We opine that it is problematic that there are nearly no criteria provided. It is dangerous or at least it might be perceived that the documentation that has to be kept by data

	of the costs, particularly for large controllers and those processing data as a main activity. The UK estimate that as a minimum large controllers and small controllers regularly processing personal data could face this cost at least once a year. The cost of obtaining prior authorisation and consultation for processing is also likely to be additional to this), FI (Seems to be overregulation. As it stands it appears that this paragraph stipulates that the controller has to act in accordance with the Regulation), DK (There are no exemptions in this article or article 11 from the obligation to adopt a policy for e.g. low-risk processing by SMEs or even natural persons), SI **YES**: CZ (Yes for large as regards policies in (1), otherwise 5(f) is repeated Specific duties in (2) dealt with in relation to relevant Articles), HU (But only if the policies to be adopted and appropriate measures to be implemented are determined on the basis of the level of risk to the rights and freedoms of data subjects presented by						controllers is a sort of replacement for the existing "notification duty" of data controllers, but even more burdensome as such (especially taking into account Article 28 of the Draft Regulation). There are sets of other rules from employment law, taxation law, customs law etc. that also require keeping of documentation, so there might be some overlaps and conflicts in application - legal non-clarity that shall produce additional administrative burdens. Also, designating/instituting data protection officers is an administrative, employment

	the data processing operations), PT, RO, MT, LU (accountability principle, link with impact assessment in article 33?)						and general costs related burden and is not acceptable as an obligation)
2. The measures provided for in paragraph 1 shall in particular include: **(a)** keeping the documentation pursuant to Article 28;	**NO**: BE, FI, MT, LU (measures should not be cumulative for all controllers) **YES**: RO MT ((28.2(g) cannot be maintained)	**NO**: RO, MT **YES**: LU	**NO**: RO **YES**: MT, LU	**NO**: RO, MT	**NO**: RO, MT	**NO**: RO, MT	BE (Considers that the reference to articles 28, 30, 33, 34 and 35 is problematic. All those articles are considered by BE as disproportionate administrative burden)
(b) implementing the data security requirements laid down in Article 30;	**NO**: FI **YES**: RO, MT	**NO**: RO, MT	**NO**: RO **YES**: MT	**NO**: RO, MT	**NO**: RO, MT	**NO**: RO, MT	
(c) performing a data protection impact assessment pursuant to Article 33;	**NO**: FI **YES**: RO, MT	**NO**: RO, MT	**NO**: RO, MT	**NO**: RO **YES**: MT	**NO**: RO, MT	**NO**: RO, MT	**NO**: RO
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	**NO**: FI **YES**: RO, MT	**NO**: RO, MT	**NO**: RO **YES**: MT	**NO**: RO, MT	**NO**: RO, MT	**NO**: RO, MT	
(e) designating a data protection officer	**NO**: FI	**YES**: RO	**YES**: RO	**YES**: RO, MT	**YES**: RO, MT	**YES**: RO	**YES**: RO

pursuant to Article 35(1).	**YES**: RO, MT	**NO**: MT	**NO**: MT			**NO**: MT	
3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.	**NO**: BE, EE, FI, MT **YES**: RO, LU (in principle, but more proportionality needed) MT (*Apart from being difficult to verify 28.2(g), it will be expensive to involve internal or external auditors)*	**YES**: FI, RO, MT **NO**: EE **YES**: LU	**YES**: EE, RO, MT, LU	**YES**: EE, RO, MT, LU	**YES**: EE, RO, MT	**YES**: EE, RO, MT	BE (Considers that this paragraph is not clear. There is a lack of predictability. BE asks COM to delete this paragraph)
Article 28 **Documentation** **1.** Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.	**NO**: BE, BG, CZ (For small: even with (4), as small tradesmen are not covered by (a) nor (b). For large: but (2) may be streamlined), DE, EE, ES, IE, IT (The obligation to retain all documentation relating to processing carried out would impose a disproportionate burden if applied to all data administrators. On the other hand, the criteria laid down in paragraph 4 of this article do not seem sufficient to introduce nuances to this obligation, and it would therefore be preferable to introduce	**YES**: BG, CZ (Larger entities may bear the burden more easily), LT, RO, LU (but with other criteria such as the risk of processing) **NO**: DE, EE, ES, FR, IE, IT, HU (The sheer size of the data controller seems quite irrelevant with regard to the potential risks stemming from certain data processing activities that might affect the data subjects), NL (The size of the entity processing the personal data is not an appropriate criterion for the application of data protection rules),	**NO**: BG **MAYBE**: CZ **YES**: DE, EE, FR, IE, IT, LT, HU, NL, PT, NO, SE, RO, MT, DK, LU (exceptions for low-risk processing) ES (In some cases and depending)	**YES**: BG, IT, LT, HU, NL, RO **PARTIALLY**: CZ (ancillary) DK, DE, SE (See general remarks) **NO**: EE, ES, FR, PT, NO, MT	**YES**: BG, IT, LT, HU, NL, RO **PARTIALLY**: CZ (ancillary) DK, DE, SE (See general remarks) **NO**: EE, ES, FR, PT, NO, MT	**YES**: BG, IT, HU, NL, PT, RO **NO**: CZ, EE, FR, LT, NO, MT DK, DE, SE (See general remarks) ES (In some cases and depending on accountabi-lity based approach)	**BE** (It is disproportionate to ask the controller and the processor to maintain documentation of all processing operations. 28.1 Each controller ***~~and processor~~*** and, if any, the controller's representative, shall maintain documentation of ***~~all~~ the main categories of*** processing ***~~operations~~*** under its responsibility)

	criteria similar to those suggested for Article 22. The exemption from the obligation to retain documentation for "*a natural person processing personal data without a commercial interest*" should be coordinated with the reference to the application of the system to natural persons (Article 2(2)(d)), LT (Subparagraphs g-h of the Paragraph 2), HU (The one-size-fits-all model might be disproportionate, a risk-based approach is needed instead), NL, SE (The obligation to keep extensive documentation on all processing operations seems overly burdensome. The exemptions, although welcome, seem insufficient), UK (This is far more burdensome that the current Directive due to the requirement to maintain documentation of all processing activities and to document all joint controllers and processors. A large	PT, NO, MT DK, SE (See general remarks) UK (SMEs whose processing is 'ancillary' to their main activity are exempt from the requirement to document all processing. However, the current wording makes it difficult to evaluate who would be captured by this, and so micros and SMEs would still need to pay for legal advice to understand what documentation they need to keep) SI (It is probably unclear, judging from the text of paragraph 4, subparagraph (b) - who is really exempted. It is also not certain that the exemption criteria do "fit". Orientation towards the possible concept of risky data would be preferable)					**BG** (Categories of recipients and possible data transfers) DK, DE SE (See general remarks) **ES** (Accountabi-lity based approach) IT (Outcome of impact assessment (where appropriate)) **HU** (• the legal basis of data processing (processing based on MS or union law vs. processing based on consent) • the source of personal data (data subject vs. third party) • the type of the processed personal data (sensitive/biome

	insurance company and a technology company were among several organisations responding to the UK Call for Evidence which described this article as 'very onerous'. The cost of this article is discussed above), MT, DK (The obligation to keep extensive documentation on all processing operations is too burdensome. The exemptions seem insufficient), LU (not "all processing" (particularly for SMEs), SI **YES**: LT (Paragraphs 1 and 3; Subparagraphs a-f of the Paragraph 2) LT (The obligation to maintain documentation of all processing operations is beneficial both for the data subject and supervisory authorities. Subparagraphs g-h of the Paragraph 2 of the Article 28 introduce far-reaching documentation obligations that creates more administrative burden and compliance						tric data vs. non-sensitive/non-biometric data) • the means of data processing (automated vs. manual) **NL** (Risks can be specified according to underlying principles or values, such as: • risks mentioned in Article 33, para 2, • risk of ID theft when data are disclosed significant damage to personality, moral standing etc. • significant financial damage breach of confidence which is protected by privileged

	costs for companies without a proportionate privacy benefit), PT NO (We support a general obligation to maintain documentation of processing activities, in particular with regard to documentation as referred to in subparagraphs (a) to (e). Regarding subparagraphs (f) to (h), we are more in doubt as to the necessity of documentation. We also believe the article should be supplemented by specific exemptions, which could be provided either at national level or in the text of the Regulation), RO FI (In principle the core idea seems acceptable. However, the formulation "shall maintain documentation of <u>all</u> processing operations" concerns FI delegation. It seems like this could be defined more precisely) MT (2(g) below cannot be maintained)						communications (such as physicians, lawyers etc)) **NO** (A general obligation to maintain documentation could be supplemented by specific exemptions, e.g. based on categories of data which are commonly processed and the processing of which does not represent any substantial risk) UK (Support a reduction in the administrative burden that this places on all controllers by dropping the requirement to document all processing, and dropping the requirement to list joint controllers and

							processors) SI (As already stated above, it seems that the documentation duty seems to be a sort of mechanical replacement for the abolished institute of the "notification duty" of data controllers)
2. The documentation shall contain at least the following information: **(a)** the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	**NO**: BE, EE **YES**: FI LU ((g) is problematic)	**NO**: EE	**YES**: EE, LU (exceptions for low-risk processing)	**NO**: EE	**NO**: EE	**YES**: EE	**BE** (28.2. **Such** documentation shall contain ~~at least~~ the following information: (a) the name and contact details of the controller, or any joint ~~controller or processor~~, and of the representative, if any;)
(b) the name and contact details of the data protection officer, if any;	**YES**: FI						BE ((b) the name and contact details of the data protection **organization or data protection** officer, if any;)
(c) the purposes of the	**YES**: FI						BE ((c) the

processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);							**generic** purposes of the processing, ~~including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);~~)
(d) a description of categories of data subjects and of the categories of personal data relating to them;	**YES**: FI						BE ((d) a description of categories of data subjects and of the categories of personal data relating to them;)
(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;	**YES**: FI						BE ((e) the ~~recipients or~~ categories of recipients of the personal data~~, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them~~;)
(f) where applicable, transfers of data to a third country or an international organisation, including	**YES**: FI						BE ((f) where applicable, transfers of **personal** data to a third country or an

the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;							international organisation, ~~including the identification of that third country or international organization~~ and, in case of transfers referred to in point (h) of Article 44(1), ~~the documentation of appropriate~~ **a reference to** safeguards **employed**;)
(g) a general indication of the time limits for erasure of the different categories of data;	**YES**: FI MT (Cannot be maintained)						BE ((g) a general indication of the time limits for erasure **or data retention policy applicable to** the different categories of data;)
(h) the description of the mechanisms referred to in Article 22(3).	**YES**: FI MT (See comments on 22.3 above)						BE (~~(h) the description of the mechanisms referred to in Article 22(3).~~)
3. The controller and the processor and, if any, the controller's representative, shall make the	**YES**: BE, FI						

documentation available, on request, to the supervisory authority.							
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors: **(a)** a natural person processing personal data without a commercial interest; or	**NO**: BE **YES**: FI	**YES**: LU (but with other criteria)	**YES**: LU				BE (The distinction should not only be based on the number of the employees but on the quantity and the quality of the data processed)
(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	**YES**: FI (Is it really necessary to exclude organisations employing fewer than 250 persons from the scope?), RO		**YES**: RO			**YES**: RO	
Article 31 **Notification of a personal data breach to the supervisory authority** **1.** In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after	**NO**: BE, DE, EE, ES (Should be redrafted on some important points), IE, HU (Except para. 4). (The one-size-fits-all model might be disproportionate, a risk-based approach is needed instead), NL, SE (The obligation to notify all data breaches is obviously disproportionate. Only	**YES**: BG **PARTIALLY**: CZ (Larger entities may bear the burden more easily) **NO**: DE, EE, ES, FR, IE, IT, LT, HU (The sheer size of the data controller seems quite irrelevant with regard to the potential risks stemming from certain	**YES**: BG, DE, EE, ES (But should be redrafted), FR, IT, LT, HU, NL, PT, NO, SE, DK **NO**: CZ, IE, RO, MT	**YES**: BG, EE, IE, IT, LT, HU, NL, NO, LU **NO**: CZ, ES, FR, PT, RO, MT DK, DE, SE (See general remarks)	**YES**: BG, DE, EE, ES (With some redrafting), IT, LT, HU, NL, NO, LU **NO**: CZ, FR, PT, RO, MT DK, SE (See general remarks)	**NO**: BG, CZ, EE, FR, NO, RO, MT DK, DE, SE (See general remarks) **YES**: ES (With some redrafting), IT, LT, HU, NL, PT	**BE (**Considers that the notion of personal data breach is not clear. **31.1** In the case of a personal data breach, **causing significant breach to the data subject,** the controller shall without

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.	serious breaches should need to be notified. Amendments are needed regarding the time limit and the amount of information required), UK (Not proportional. This is expected to be very costly to businesses. UK survey evidence finds 11% of small businesses and 45% of large businesses had at least one incident in the past year where data protection laws were breached (that is a minimum of 22,600 breaches)[1]. The cost of reporting (including dealing with responses from the Commissioner) is estimated to be £1,000 to £2,000 and there is an additional cost through 'damage to reputation' of £100-£1,000 to a small businesses, and £5,000-£40,000 for a large business. Data controllers have also reported that 24 hours is not a realistic reporting deadline; for example, in the UK	data processing activities that might affect the data subjects), NL (The size of the entity processing the personal data is not an appropriate criterion for the application of data protection rules), PT, NO, RO, MT DK, SE (See general remarks)					undue delay ***after the establishment of the existence of a personal data breach*** ~~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.~~ **The notification of a personal data breach to the supervisory authority shall not be required if the controller has implemented appropriate technological protection measures, and**

[1] PWC (2012), 'Information security breaches survey: technical report'.

	Call for Evidence one large telecommunications company reported that it takes a minimum of 72 hours to determine the details of the breach, while an organisation representing retailers estimated that it can take several days or weeks to conclude the preliminary investigation), DK (The obligation to notify all data breaches is disproportionate. Only serious breaches should need to be notified. Amendments are needed regarding the time limit and the amount of information required), LU (not in 24 hours and not for all data breaches, a threshold needs to be defined), SI **YES**: BG, CZ (For small: (1) Time limit and justification excessive. Should be replaced by ex-post notification. For large: (1) Time limit and justification excessive.						**that those measures were applied to the data concerned by the personal data breach causing significant breach to the data subject. ~~Such technological protection measures may include those that render the date unintelligible, unusable or anonymised to any person who is not authorised to access it.~~)** BG (A criterion for severity of data breach should be included (the supervisory authority should be informed only in case of severe data breaches – e.g. affecting high number of individuals or in case of high

	Should be replaced by ex-post notification), IT, HU (Only with regard to the obligation to document personal data breaches – para. 4), PT, FI (The obligation to notify appears proportional. However, red together with the definition of the personal data breach, it does seem to contain all the smallest personal data breaches as well. It would seem more appropriate to limit this to the notable or significant personal data breaches), RO, MT, LU (Agree on principle) LT (The introduction of this obligation is welcome as it may help to ensure security of data processing, however it is impossible evaluate if it is proportional, since the criteria and requirements for establishing a data breach are not specified in the Regulation)						public interest) **DK, DE, SE** (See general remarks) **ES** (Accounta-bility based approach) **IT** (Criteria to be developed by EU bodies (ENISA + EDBP) **HU** (• the legal basis of data processing (processing based on MS or union law vs. processing based on consent) • the source of personal data (data subject vs. third party) • the type of the processed personal data (sensitive/biom etric data vs. non-sensitive/non-

	NO (We support a general obligation to notify in cases of a personal data breach, but believe one or more *de minimis* exemption(s) should be provided. Such exemptions could be given either at national level or in the text of the Regulation)						biometric data) • the means of data processing (automated vs. manual) **NL** (Risks can be specified according to underlying principles or values, such as: • risks mentioned in Article 33, para 2 • risk of ID theft when data are disclosed • significant damage to personality, moral standing etc. • significant financial damage breach of confidence which is protected by privileged communications (such as

							physicians, lawyers etc) UK (Only serious breaches should be notified, without a time limit. Serious breaches should be defined according to the amount of personal data that is processed and the sensitivity of that data) MT (Threshold to be amended to 48 hours) **YES**: LU SI (Too early from the contents and systemic viewpoints to have a semi-stabilised position)
2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately	**NO**: BE, EE **YES**: FI, MT	**NO**: EE, MT	**YES**: EE **NO**: MT	**YES**: EE **NO**: MT	**YES**: EE **NO**: MT	**YES**: EE **NO**: MT	

after the establishment of a personal data breach.							
3. The notification referred to in paragraph 1 must at least: **(a)** describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;	**NO**: BE, EE **YES**: FI (The aim to notify the supervisory authority without undue delay is welcome. This should not be compromised with notification requirements which are difficult to accomplish. It would seem to suffice at that stage to describe the nature of the personal data breach and to tell the measures proposed or taken to address the personal data breach and consequences of the personal data breach known at that stage), MT, LU (but (c) and (d) only for serious breaches, or "where possible". Point (d) should be limited to describing "technical" consequences)	**NO**: EE, MT	**YES**: EE **NO**: MT	**YES**: EE **NO**: MT	**YES**: EE **NO**: MT	**YES**: EE **NO**: MT	
(b) communicate the identity and contact details of the data protection officer or other contact point	**YES**: FI						

where more information can be obtained;							
(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	**NO**: FI						
(d) describe the consequences of the personal data breach;	**NO**: FI, NO (We suggest that a more flexible wording is chosen, e.g. by adding the words "if possible")						
(e) describe the measures proposed or taken by the controller to address the personal data breach.	**YES**: FI						
4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the	**NO**: BE, EE, LU (Not all breaches, a threshold is needed) **YES**: FI (As previously in Article 31(1)), MT	**NO**: EE, MT	**YES**: EE **NO**: MT	**YES**: EE, LU **NO**: MT	**YES**: EE, LU **NO**: MT	**YES**: EE **NO**: MT	**BE** (Considers that the notion of personal data breach is not clear)

information necessary for that purpose.							
Article 32 Communication of a personal data breach to the data subject **1.** 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 referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	**NO**: BE, BG (Insofar small controllers will be challenged when exercising this obligation which should be adapted to the amount of data, the risk of processing and the number of individuals), CZ (For small: Should focus on damage prevention first. Breach should be notified to other entities for damage prevention. Other information only subsequently. For large: Should focus on damage prevention first. Breach should be notified to other entities for damage prevention. Other information only subsequently), DE, ES (Depending on cases), NL, SE (Only serious breaches should need to be notified. Amendments are required), DK (Only serious breaches should need to be notified)	**YES**: BG (Insofar the criterion for the cases in which individuals should be notifies is not specified which will burden the small controllers) **PARTIALLY**: CZ (Larger entities may bear the burden more easily) **NO**: DE, EE, ES, FR, IT, LT, HU (The sheer size of the data controller seems quite irrelevant with regard to the potential risks stemming from certain data processing activities that might affect the data subjects), NL (The size of the entity processing the personal data is not an appropriate criterion for the application of data protection rules), PT, NO, RO, MT DK, SE (See general remarks)	**YES**: BG, CZ (Sensitivity of data, Damage prevention), DE, EE, FR, IT, LT, HU, NL, PT, NO, SE, DK ES (It depends on circumstances) **NO**: RO, MT	**YES**: BG, EE, IT, LT, HU, NL, LU **NO**: CZ, ES, FR, PT, NO, RO, MT DK, DE, SE (See general remarks)	**YES**: BG, EE, IT, LT, HU, NL, LU **PARTIAL-LY**: CZ (Damage caused to many people) ES (It depends on circumstances) **NO**: FR, PT, NO, RO, MT DK, SE (See general remarks)	**NO**: BG, CZ, FR, LT, HU, PT, NO, RO, MT **YES**: DE, EE, IT, NL ES (It depends on circumstances) DK, SE (See general remarks)	**BE** (Considers that the notion of personal data breach is not clear. 32.1 When the personal data breach is **causing significant breach to the data protect** ~~likely to adversely affect the protection of the personal data or privacy of the data subject~~, the controller shall, ~~*after the notification referred to in Article 31,*~~ communicate the personal data breach to the data subject without undue delay) **BG** (We consider the notification criterion for very unclear- "the possibility

	YES: IE, IT, HU (But only in case of serious breaches, when it is inevitable to inform the data subjects in order to make them able to mitigate the adverse effects. These cases should be defined in the legal instrument more precisely), PT, NO, FI (1) The attempt to qualify *the affect the protection of the personal data or privacy* is welcome), RO, MT, LU LT (Since the circumstances in which a data breach should be notified are not specified in the Regulation, there are no possibilities to evaluate if this obligation is proportional)						for negative impact on the personal data protection" and it should be specified in order to reduce the administrative burden) **DK, DE** (See general remarks)[1] **HU** (• the legal basis of data processing (processing based on MS or union law vs. processing based on consent) • the source of personal data (data subject vs. third party) • the type of the processed personal data (sensitive/biometric data vs.

[1] **DE**: The introduction of a more appropriate threshold value should be examined. If directly notifying all data subjects is not possible or would create a disproportionate burden, public notification or another equally appropriate notification method should be possible instead.

							non-sensitive/non-biometric data) • the means of data processing (automated vs. manual) **NL** (Risks can be specified according to underlying principles or values, such as: • risks mentioned in Article 33, para 2 • risk of ID theft when data are disclosed • significant damage to personality, moral standing etc. • significant financial damage breach of confidence which is protected by privileged communica

							tions (such as physicians, lawyers etc) LU (Risk for identity theft or financial loss)
2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).	**NO**: BE **YES**: FI	**NO**: EE	**YES**: EE	**YES**: EE	**YES**: EE	**YES**: EE	BE (See comment above) ES (Accountability bases approach) IT (Risk assessment criteria as developed by EU bodies (ENISA + EDBP)
3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures,	**NO**: BE **YES**: FI (The underlying idea seems good. However, this provision should be further formulated), LU						BE (See comment above) SE (See general remarks)

and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.							
4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.	**NO**: BE **YES**: LU						BE (See comment above)

ARTICLE OF DRAFT DP REGULATION	PROPORTIONALITY PRINCIPLE	CRITERIA PROPOSED IN DRAFT DP REGULATION (not mutually exclusive)		OTHER/ADDITIONAL POSSIBLE CRITERIA (not mutually exclusive)			
	Proportionality Test – is the obligation proportional, particularly in terms of the burden it imposes on micro, small, and medium-sized enterprises as compared to large enterprises? (YES/NO)	**Is the size of the entity processing the personal data an appropriate criterion for the application of data protection rules in this case? (YES/NO)**	**Risk involved in the processing activities (e.g. sensitivity of data, systematic monitoring of data subjects) (YES/NO)**	**Volume of personal data processed (YES/NO)**	**Number of data subjects affected (YES/NO)**	**Which category of data subjects is affected (e.g. minors) (YES/NO)**	**Other (please specify)**
Art. 6.1(f)	**NO:** MT (Not all processing operations are covered by specific laws. Legitimate interests therefore need to apply also to public authorities)	**NO:** MT	**NO:** MT	**NO:** MT	**NO:** MT	**NO:** MT	
Art. 7(2)	**NO:** EE	**NO:** EE	**YES:** EE	**YES:** EE	**YES:** EE	**YES:** EE	
Art. 7(4)	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	
Art. 8(1)	**NO:** EE						
Art. 8(3)	**YES:** PL	**NO:** PL	**YES:** PL	**YES:** PL	**YES:** PL	**YES:** PL	
Art. 16	**NO:** EE	**NO:** EE	**YES:** EE	**YES:** EE	**YES:** EE	**YES:** EE	EE (The assessment to the stipulation depends on how often the completion of incomplete personal data can be requested. We suggest that the incomplete personal data should only be revised, when it is necessary to complete data processing purposes (therefore, only in essential issues)

Art. 17	**NO**: BE **YES**: RO	**NO**: RO	**NO**: RO	**NO**: RO	**NO**: RO	**NO**: RO	BE (Waits for the new proposition of COM on this article)
Art. 17 (2)	**NO:** EE	**NO:** EE	**YES:** EE	**NO:** EE	**NO:** EE	**YES:** EE	
Art. 17 (4a)	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	EE (Might be translation problem, but it is necessary to avoid that the stipulation puts an obligation to the controller to verify the accuracy of the data (in Estonian kontrollima), since it is unclear, what are the possibilities for a controller to actually control the accuracy of the data)
Art. 17 (6)	**NO:** EE	**NO:** EE	**YES:** EE	**NO:** EE	**NO:** EE	**YES:** EE	
Art. 17 (7)	**NO:** EE	**NO:** EE	**YES:** EE	**NO:** EE	**NO:** EE	**YES:** EE	
Art. 18	**NO**: BE, RO **YES**: RO	**NO**: RO	**NO**: RO	**NO**: RO	**NO**: RO		BE (Underlines the difficulties to apply this right to the public sector. Considers that this point is problematic regarding intellectual property rights. Asks to delete the words « and any other information » and asks COM to explain in a recital that only data provided by the data subject should be given back. Wants to be assured that the aggregated data will not be transmitted)
Art. 19 (3)	**NO:** EE	**NO:** EE	**YES:** EE	**NO:** EE	**NO:** EE	**YES:** EE	EE (Processing of personal data can be vital to a business or the public sector, therefore this should be allowed only in special/extraordinary cases)
Art. 20 (4)	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	EE (The data should be provided upon request, not pre-emptively)
Art. 22 (4)	**NO:** PL	**NO:** PL	**YES:** PL	**YES:** PL	**YES:** PL	**NO:** PL	
Art. 23 (1,2)	**YES:** EE	**YES:** EE	**YES:** EE	**YES:** EE	**YES:** EE	**YES:** EE	EE (depends whether the obligation will be applied retroactively or in the future. It should be proportional for SMEs.)
Art. 25	**YES**: IT	**NO**: IT (no rationale behind excluding appointment of a EU representative based on the size of the	**YES**: IT	**YES**: IT	**YES**: IT	**YES**: IT	

		enterprise (Article 25(2)b.) as such appointment is meant to enable exercise of data subjects' rights (see above remarks). Accordingly, Article 25(2)b. should be deleted or worded differently by having regard to risk factors)					
Art. 25 (2)	**YES:** PL	**NO:** PL	**YES:** PL	**YES:** PL	**YES:** PL	**NO:** PL	
Art. 26 (3)	**NO:** EE	**NO:** EE	**YES:** EE	**NO:** EE	**NO:** EE	**NO:** EE	
Art. 30:	**YES**: NL	**NO**: NL	**YES**: NL	**YES**: NL	**YES**: NL	**YES**: NL	
Art. 33	**NO**: BE						BE considers that the definition of "specific risks" is unclear and extremely broad. A definition of processing operations that present specific risks is needed. 33.1. Where processing operations differ consistently from existing practices of the Controller and the new approach in itself presents specific risks creating doubts with the compliance of this Regulation, 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. 2. The following processing operations in particular present specific risks referred to in paragraph 1: a) a systematic and extensive evaluation of personal aspects relating to a natural

							person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which ~~measures~~ **decisions** are based that produce legal effects **that gravely and adversely affect the individual's fundamental rights** ~~concerning the individual or significantly affect the individual~~; 33.3 Delete 33.4 Delete
Art. 33 (1 a, e) + 34 (6)		**NO:** EE	**NO:** EE	**YES:** EE	**YES:** EE	**YES:** EE	
Art. 33 (1-c)	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	EE (Additional criteria that would make this point proportional is the location of the surveillance equipment)
Art. 34	**NO**: BE, NL (The requirement of prior authorisation and prior consultation should be linked to the risks mentioned in Article 33, para 2, and to other associated risks.						BE (Considers that this article leads to a disproportionate administrative burden not only for the controller or the processor but also for the DPA's)
Art. 33 (6)	**YES:** PL	**NO:** PL	**YES:** PL	**YES:** PL	**YES:** PL	**YES:** PL	
Art. 34 (2)	**NO:** EE	**NO:** EE	**YES:** EE	**YES:** EE	**YES:** EE	**YES:** EE	
Art. 34 (4)	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	EE (Potential impact can be disproportional)
Art. 34 (5)	**NO:** EE	**NO:** EE	**YES:** EE	**YES:** EE	**YES:** EE	**YES:** EE	
Art. 34 (7)	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	**NO:** EE	

Art. 35	**NO**: EE, NL (Size of an entity is not an appropriate criterion for the application of data protection legislation The requirement to designate a Data protection officer should be linked to the risks mentioned in Article 33, para 2, and to other associated risks).	**NO**: NL	**YES**: NL, EE	**YES**: NL, EE	**YES**: NL, EE	**YES**: NL, EE	
Art. 35 (1)	**YES:** PL	**YES:** PL	**YES:** PL	**YES:** PL	**YES:** PL	**YES:** PL	
Art. 35 (7)(8)	**NO**: IT	**NO**: IT	**YES**: IT	**YES**: IT	**YES**: IT	**YES**: IT	
Art. 79 (3)	**YES:** PL	**YES:** PL	**YES:** PL	**YES:** PL	**YES:** PL	**YES:** PL	

ADDITIONAL COMPLIANCE COSTS

CZECH REPUBLIC

Article 2(d) fossilises too large compliance costs for individuals by keeping only the old "household exemption". Simple and easy rules for small processing are needed.

Article 4(8) raises compliance costs by requiring "explicit" consent

Article 8 raises compliance costs by requiring identifications and verifications that may or may not be practicable.

Article 11(1) raises compliance costs especially for small and off-line entities (such as small bakers).

Article 17 raises compliance costs due to its extent (electronic, hard copy) and due to breadth of third parties in (2).

Article 18 raises compliance costs by requiring portability. It may be that such requirement would reduce costs on the part of data subjects and open market better, but at least the scope of article should be defined more precisely.

Articles 33 – 34 raise compliance costs by convoluted and unclear regulation of impact assessments and prior authorizations/notifications and related duties, such as to seek opinions of data subjects.

Articles 35 – 37 raises too large compliance costs by requiring Data Protection Officers.

This short list is for orientation purposes only and CZ reserves the right to designate other provisions (in particular provisions not yet discussed) as presenting compliance costs, administrative burdens or other prosperity-damaging issues in future.

GERMANY

At present, Germany cannot see how the draft Regulation, as it currently stands, can actually lead to a reduction in red tape. Some relief can be expected, e.g. as a result of the elimination of the comprehensive notification requirement. However, a considerable extra financial burden would be placed on the economy by the currently planned scope of and any further increase in the right to data portability (Article 18), the information and documentation requirements (Articles 14, 15 and 28), the organisational requirements (Articles 12 and 18), the data processing impact assessment (Article 33) and the prior authorisation from and/or consultation of the supervisory authority as set out in Article 34. For several other sectors (e.g. statutory health insurance), the possibility cannot be ruled out that their proper functioning could be jeopardised. The proposed EU Regulation must therefore be revised – particularly in view of the risk criteria specified in the questionnaire – in order to strike an appropriate balance between the protection of personal data and the free movement of personal data within the EU. Further risk criteria should be established. In the public sector and in the health care sector, Member States should be able to retain room for manoeuvre, particularly in order to provide for higher standards of protection.

SPAIN

As previously stated[1], other provisions do contain additional compliance costs.

1.1 Art. 20

Art. 20.4 in relation to art.14 includes additional information to be provided in the context of profiling. Depending on the context and on the interpretation it could lead to excessive compliance costs.

[1] See 1.1

1.2 Art. 23

Paragraph 23.1 could cause unreasonable burden depending on context and on interpretation.

1.3 Art. 33

Impact assessments could add important costs to the controller (or the processor if it is the case). This provision should be reconsidered under the scope of the accountability principle. According to this idea, codes of conduct and certifications policies could aid in order to diminish the financial impact without putting privacy at risk.

Processing operations that require impact assessment should be reconsidered as well.

1.4 Art. 34

The need of authorization or consultations should be reconsidered under the scope of the accountability principle and according to results previously obtained in art. 33.

The existence of certifications, DPO, and/or codes of conduct should lead to a clear diminution of the prior authorizations and consultations cases.

1.5 Arts. 35-37

The existence of a data protection officer adds with no doubt value in terms of security and lawfulness. This should allow reasonable compensations in terms of administrative and bureaucratic burdens; otherwise the data protection officer might create undesirable costs in both public and private sector.

1.6 Chapter V

International transfers should be simplified in terms of bureaucratic burdens.

Authorizations of contractual clauses should not be needed provided that the controller has a DPO or a proper certification for transfer purposes.

Capacities should be assured as well in order to avoid large periods for adequacy processes. Partial adequacy decisions, as foreseen in the draft regulation, should not be enough in order to reduce timing if proper capacities are not assured.

1.7 Chapter VII

Consistency mechanism should be simplified. According to its current design it is much long lasting and the intervention of the Commission should be deleted.

SLOVENIA

Issue of fines for administrative sanctions

Drafted provisions on fines for administrative sanctions seem to be tailored for big enterprises (global data controllers from the information technology sector) and seem to project the viewpoint that the area of data protection is a competition law matter, which is again unacceptable, since data protection starts form the viewpoint of human rights (of a natural person) and in some cases also from the corpus of national constitutional law. Also, due to the high amounts of drafted fines they might become a tool for unnecessary and unfair bankruptcies. They are also unacceptable from the viewpoints of principles of proportionality and subsidiarity. Starting solely from the viewpoint of the development of the area of data protection it is questionable, why was this "punitive mode" selected, supervision over protection of personal data is namely logically oriented towards developing the culture of data protection - providing advice, enforcing or accepting voluntary or binding corrective measures, while repression should be provided only when the ultima ratio principle in this context shows this as a very advisable or necessary solution. However, we do accept the need to provide for stating general rules of (substantive) elements of administrative offences in this draft legal act.

Issue of data protection officers

From the systemic and functional approaches we assess at the moment that data protection officers have not been shown yet as adding recognizable added value in practice, especially from the modes of preventing data security breaches, violations of privacy and human dignity rights and/or "whistle-blowing" actions, so we oppose their obligatory (!) introduction. But also, from the important viewpoints of costs and economic capacities, their obligatory introduction would be also unacceptable.

Also, another problematic viewpoint might be debatable - is it maybe possible to assess (at least in a academic manner) that the proposed introduction of obligatory data protection officers, with duties allocated to them and conditions attached to their status and conditions attached to their employers, might mean an establishment of a new legal profession, or at least a partial legal profession, that is also a partially regulated profession? Is such special regulation in this legal setting acceptable?

UNITED KINGDOM

Data Protection Officers

Most large data controllers in the UK have a team responsible for data protection. Appointing one person to the role of DPO will be costly, due to the need to provide new contractual arrangements to meet the requirements of the Regulation. The UK estimates that 42,000 micro and SMEs (4%) in the UK will be affected by the DPO requirement due to the nature of their processing. This will cost micros and SMEs £34 - £182 million p.a. (€42m-€228m). The lower bound estimate is based on four hours of legal validation work, as per the EU Commission Impact Assessment, while the upper bound assumes that all medium enterprises affected (3,000) will need to employ a full-time DPO.

Data Protection Impact Assessments

It is estimated that for the UK they are 42,000 micros and SMEs that will be required to carry out DPIAs based on their nature of their processing, and that all large data controllers will need to carry out DPIAs. Using survey data on the number of organisations carrying out security risk assessments, it is estimated that only 11% of large organisations and 26% of small organisations are not already doing these[1]. Based on this data, the additional cost to business is estimated to be £67 - £81 million (€84m-€101m), depending on whether or not micro organisations need to carry out DPIAs at all. This is a conservative estimate as it assumes data controllers do only one assessment a year, whereas in practice they are likely to need to do far more.

There will also be additional costs to controllers already carrying out DPIAs as article 33 includes a requirement to consult data subjects in the impact assessment.

Consent, profiling and definition of personal data (article 4 and 20)

The requirement for consent to be explicit (art. 4), the restriction on profiling (art. 20) and extending the scope of personal data to include online identifiers (art. 4), are together likely to extremely detrimental to growth in the technology sector, due to the restrictions they place on direct marketing. Web services, such as search engines, are able to be provided free of charge because they generate revenue through personalised advertising. Growth in behavioural advertising has also been beneficial for growth in the advertising sector and the businesses whose products they are marketing; in the UK in 2011 online advertising was the biggest source of advertising revenue in the UK after TV and is expected to continue to grow[2].

1 PWC (2012), Information security breaches survey: technical report.
2 Demos (2012), 'The Data Dialogue'.

The limitations that the Regulation places on direct marketing are therefore expected to be extremely costly to business. In the UK Call for Evidence, one advertising agency estimated that the proposals as drafted may cost the UK £633 million in lost advertising revenues as companies reduce their advertising expenditure, while DMA found the cost to business to be £47 billion if businesses could no longer use web analytics for marketing purposes[1].

Data portability and the right to be forgotten

These articles are expected to be costly to implement if to the need for businesses to modify their IT systems in order to ensure they are compliant. In the UK Call for Evidence, one marketing company estimated that data portability and right to be forgotten clauses could require a one off system development costing £100,000, while a large telecommunications company estimated that data protection by design, data portability and the right to be forgotten would cost £5 million.

High Sanctions

The level of fines are disproportionate to the harm caused, for example 0.5% of turnover for failing to comply with a SAR request, and so in some cases could drive a marginal firm out of the market. High sanctions create a risk adverse attitude among small controllers, leading to additional costs of employing legal advice to ensure they are compliant.

---

[1] DMA (2012), 'Putting a price on direct marketing.