Fedil
Business Federation
Luxembourg

Fedil – Business Federation Luxembourg

Comments on the Commission Proposal for a Regulation on the Protection of Personal Data in the EU and on the free Movement of such Data

7, rue Alcide de Gasperi
Luxembourg-Kirchberg
Boîte postale 1304
L-1013 Luxembourg

E-mail fedil@fedil.lu
Téléphone +352 43 53 66-1
Fax +352 43 23 28
www.fedil.lu

Table of Contents

Introduction

Fedil-Business Federation Luxembourg acting as a multi-sector business federation in Luxembourg welcomes the European Commission's proposal for a General Data Protection Regulation published on 25th of January 2012 as it has the potential to ensure a consistently high level of data protection throughout the EU while at the same time facilitating the free flow of information in the Internal Market. In particular, we believe that the approach chosen by the Commission to introduce a fully harmonised single set of data protection rules applicable throughout the EU, coupled with a one-stop-shop enforcement mechanism, is fundamental in solving existing problems and creating a consistent regulatory level playing field across all EU Member States. Furthermore, it will help reduce administrative burdens and improve the level of trust and legal certainty to the benefit of consumers and businesses, a prerequisite for a well-functioning Digital Single Market.

The review of the EU's Data Protection Framework (the Framework) provides a unique opportunity to update and modernise the rules as well as to strengthen individuals' privacy rights while promoting the continued growth of the Internet economy, fostering innovation and trade. Striking the appropriate balance here will be critical to Europe's economy.

However, achieving the right balance will require a much more pragmatic and results-oriented approach, which truly embraces principles such as accountability, the context in which data is processed as well as the actual risks involved for individuals. Instead, the proposed Regulation pursues an over-regulatory and prescriptive approach which we fear will not only place additional unnecessary burdens and costs on companies without any benefit for individuals, but more importantly risk stifling innovation and economic growth in Europe.

We believe that the review should be guided by a fundamental principal of the EU, namely the notion of the rational and informed consumer. Any over-protective regulation will convey a perception of a consumer who is vulnerable and ultimately unable to navigate through life without the encompassing protection of the government. We are certain that such extensive notion is not intended by the EU. However, in our understanding of the proposed Regulation there are traces implying this perception. Furthermore, the far reaching powers that the proposal attributes to the European Commission through the instrument of "delegated acts", which would apply in a number of key areas, will entail legal uncertainty.

Given the direct impact of data protection rules on the information and communication technologies (ICT) sector, which is a well-established industry in Luxembourg, we would like to comment on some key issues under discussion, which we feel need to be clarified and refined to allow the new Framework to achieve its objectives and be workable in practice.

1. Territorial scope, DPA jurisdiction, one-stop-shop feature

Fedil strongly supports the introduction of a "one-stop-shop" approach with respect to the competence of the Data Protection Authorities (DPA), which is particularly crucial for multi-national companies with separate legal entities and different business lines operating in several Member States. This will reduce complexity and administrative burden for companies as they will have to interact with only one single DPA - the authority in the country where they have their main establishment. Coupled with the so-called "consistency mechanism", this will help ensuring a consistent application of data protection rules across Europe. However, we feel that in order to achieve a true one-stop-shop and avoid confusion over the determination of the "lead DPA", proposed definitions of the "main establishment" need to be clarified further. This concerns also the mutual cooperation aspects between DPAs.

a. Clarification of the "main establishment" concept

A clear understanding of the term "main establishment" is crucial as it is the decisive factor for determining which DPA should be the lead authority. We take the view that the proposed terminology is too vague, leaving too much room for diverging interpretation. In this respect, we concur with the Article 29 Working Party, which in its recent opinion 01/2012 on the data protection reform proposals has emphasised that the proposed rules require clarification.

Under the proposed definition, the term 'establishment' could be interpreted differently and therefore result in an inconsistent or more burdensome application of the one-stop-shop feature than intended. In order to avoid unnecessary confusion for businesses and DPAs as well as satisfy the need for legal certainty, the establishment definition should be interpreted based on a limited set of objective criteria. Article 54 TFEU should be the relevant starting point for determining the location of an establishment, and this term should then be narrowed further in the Regulation to determine the "main establishment" for data protection purposes. In any case, it should be clarified that the designation of establishment for data protection compliance purposes should be without prejudice to such designation for other purposes of EU law (e.g., tax, insolvency, other compliance purposes).

The Regulation introduces different terms in relation to business operations (e.g. 'management activities determining the processing purposes', 'central administration', 'economic activity', 'controlling undertaking'), which particularly for groups of undertakings makes it difficult to determine which of their entities is the 'main establishment' and may lead to several DPAs claiming jurisdiction over companies. For the sake of consistency and legal clarity for multinational groups of companies, we take the view that the Regulation should provide for a single uniform definition of 'main establishment', applicable across borders to controller and processor. Ideally, this definition should be based on a set of relevant objective criteria, which a group of undertakings can choose from in order to officially designate its location of 'main establishment' as regards to the Data Protection Law. The affirmative obligation for businesses to self-assess their structures and declare the main establishment on the basis of objective criteria is essential for eliminating disputes over main establishment.

A similar concept has already been developed under current EU Data Protection Law, namely in relation to Binding Corporate Rules (BCRs), where the 'lead' DPA responsible for the evaluation and approval of BCRs is determined on the basis of objective criteria[1]. Having set a precedent and for the sake of consistency, this concept could perfectly lend itself for the purpose of determining the place of 'main establishment' as regards to the data protection legal framework.

[1] European Commission's DG Justice Guidance on how to designate the lead authority in the framework of BCRs, accessible here: http://ec.europa.eu/justice/policies/privacy/binding_rules/designation_authority_en.htm

The objective criteria for the determination of the 'lead DPA' should primarily be the location of a group's designated European headquarter, which we understand to be the entity in the Union in which are placed certain corporate services, which for group purposes is typically considered as "shared corporate services" centre whose costs are charged to the line of businesses or borne by the parent group. They could also include, for instance, the entity within the group with delegated data protection responsibilities, the entity which is best placed, in terms of management, administrative functions etc., to deal with data protection matters, or the entity where most decisions in terms of processing operations are taken.

On the basis of such criteria, businesses should officially designate their place of 'main establishment' in the Union and such designation should apply to all entities that are part of the group established in the Union. The Regulation should also clarify that the lead DPA for the company's main establishment should be competent to supervise all the processing operations carried out by all entities of the group as far as they are subject to the Regulation.

We propose designation of the main establishment to be accomplished through a regular filing by the controller or processor with the relevant DPA. In order to ensure legal certainty and transparency, such designation should have binding effects for a specific period (e.g. three years) with exceptions and transitional rules for changes in the main establishment due to events that are unrelated to data protection compliance jurisdiction, e.g., takeovers, mergers, acquisitions and/or insolvencies. Such information would be available in real-time on a database shared by DPAs.

We do not believe that the proposed approach would lead to forum shopping for data protection purposes given all the other factors which are related to the group's decision where to locate its headquarters entity. On the contrary, we believe that such a single, consistent definition of 'main establishment', to be used for all situations, would provide the required level of legal certainty to the benefit of individuals, companies and DPAs alike. Furthermore, as the legal instrument proposed by the Commission is a regulation, the rules regarding data protection will be fully harmonised across the EU and there will be no space for regime shopping.

Fedil's recommendation:

We suggest aligning the 'main establishment' concept for the determination of the 'lead DPA' to the one developed in relation to Binding Corporate Rules. We propose that (1) groups of companies should be allowed to designate their location of 'main establishment' based on a set of objective criteria, particularly the location of the group's EU headquarters; (2) such designation should apply to all entities that are part of the group established in the Union, and (3) a transparent and binding process should be established for such designation with dispute resolution mechanism for regulators and appeal possibilities for companies.

b. Clarification of the extra-territorial reach of the Regulation

According to Article 3(2), the scope of the Regulation extends to controllers established outside of the EU where the processing activities relate to goods/services offered to EU citizens or where their behaviour is monitored. We acknowledge that it is desirable to have companies based outside of the EU respect EU data protection standards when processing personal data of EU citizens. However, we would recommend clarifying the criteria determining the scope of application of the Regulation for companies not established in the EU.

The term “offering” of goods and services cannot in our view constitute a valid legal notion in the context of cross-border activities to determine the applicable law and jurisdiction. Companies may not know that their customers are European residents and if the mere fact of “offering” goods and services was the determining criteria, then they would be obliged to process even more personal data to identify whom of their customers are EU citizens. The EU jurisprudence[2] rather suggests that applicable jurisdiction needs to be determined based on the question whether a service is intentionally addressed to EU consumers or not, and that the terms ‘targeting’ or ‘directing’ carry more legal certainty. According to the ECJ, these notions involve objective criteria such as the use of a language or a currency other than the language or currency generally used in the country in which the trader is established with the possibility of making and confirming the reservation in that other language, the mention of telephone numbers with an international code, the use of a top-level domain name with the .eu suffix or other than that, of the country in which the trader is established.

Fedil’s recommendation:

We suggest clarifying that the Regulation applies to non-EU established controllers only when they have envisaged processing personal data of data subjects residing in the Union by amending Article 3.2. (a) to replace the word ‘offering’ by ‘targeting’ or ‘directing’ goods or services and by clarifying in corresponding recitals that the mere accessibility of the controller’s website by a data subject residing in the Union is insufficient.

c. Clarification of “one-stop-shop” concept and DPA cooperation mechanisms

While Fedil explicitly welcomes the Commission’s proposals with respect to DPAs competence, we believe that further clarification is needed to ensure that the ‘lead DPA’ can truly function and operate as a one-stop-shop. Contrary to the Commission’s declared objective, the enforcement system as currently designed would not allow for such a one-stop-shop and companies are put in difficult legal situations in case of a conflict between DPAs claiming competence for a specific case.

This is particularly true in the event of a conflict between DPAs as to a DPA’s lead role. In such cases, a dispute resolution mechanism should be implemented allowing the controller to put forward its viewpoint and arguments. With a view to reduce the legal uncertainty resulting from such situation, neither DPA should be able to issue or enforce decisions (including fines) against the controller until the conflict is cleared. The controller should have the right to appeal any decision taken with respect to a DPA’s lead role as the result of the conflict resolution mechanism.

Furthermore, the Regulation seems to limit the role of the ‘lead DPA’ to the supervision of all cross-border processing activities of the controller and, where individuals in several Member States are affected, to the cooperation with the DPAs of those Member States as well as the coordination and the execution of joint investigations and enforcement actions. The role of the lead authority is unclear when another Member State’s DPA makes use of the powers granted by the Regulation (see Article 51 (1), 52, 53) and, for instance, based on a complaint conducts an investigation against a controller, whose main establishment is outside of this DPA’s territory. The Regulation is silent about any involvement of the lead authority in such cases and it is also not clear how far such a case would trigger the application of the consistency mechanism.

[2] Judgment of the Court (Grand Chamber) of 7 December 2010, Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09); Judgment of the Court (Grand Chamber) of 12 July 2011, L’Oréal SA and Others v eBay International AG and Others (Case C-324/09)

We take the view that the Regulation should clarify and strengthen the one-stop-shop concept by providing an obligation which would ensure that DPAs, who receive a complaint or wish to launch investigations for other reasons, are required to refer such matters to the lead authority and merely act as point of liaison. A real-time data base (accessible at least by all DPAs) should refer the lead DPA for each company. In any case, a DPA - not being the lead DPA- should not be able to launch actions against a company for which another Member State DPA acts as lead DPA. In such situation, the former should refer the matter to the lead DPA and hand over competence to the latter. The company should refer the matter to its lead DPA and should in no event be bound by actions or decisions taken by non-leading DPAs. As the case may be, the dispute resolution mechanism referred to in this section 1. c should apply.

Furthermore, we note that the 'lead DPA' and one-stop-shop concept as currently provided for in the draft Regulation does not apply to controllers who are not established in the EU, but would fall within the scope of the Regulation. The Regulation lacks rules on which DPA should be the lead in such cases, and consequently, such companies could be required to interact with any (or all) of the 27 DPAs depending on whether their processing operations concern individuals in their territory. In line with our proposal above, we would suggest closing this gap by granting non-EU established companies the right to designate a 'lead DPA', based on objective criteria to be further defined.

Fedil's recommendation:

1. Introduce a single uniform definition of 'main establishment', which is aligned with the concept used for the determination of the 'lead DPA' for Binding Corporate Rules and is based on a set of relevant objective criteria – particularly the location of a company's EU headquarter. Allow groups of undertakings to officially designate their location of 'main establishment' in terms of Data Protection Laws based on these criteria and ensure that such designation applies to all processing of all entities that are part of the group established in the European Union.
2. Make sure that the Regulation applies to non-EU established controllers only when they have envisaged processing personal data of data subjects residing in the EU by amending Article 3.2. (a) to replace the word 'offering' by 'targeting' or 'directing' goods or services.
3. Clarify and strengthen the "one-stop-shop" concept by providing for an obligation which would ensure that DPAs, who receive a complaint or wish to launch investigations for other reasons, are required to refer such matters to the lead authority and merely act as point of liaison.

2. Definition of personal data

The definition of personal data is a key concept triggering the application and enforcement of EU data protection law and entailing a number of obligations and liabilities for controllers and processors. Therefore, it is crucial that the definition is clear and future-proof.

The draft Regulation substantially extends the scope of data covered by it by defining personal data as "any information relating to a data subject who can be identified by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data or online identifier…". As a result of this very broad definition, the Regulation is likely to apply to the majority of all processing operations, irrespective of the context of the data processing, the risk of identification and the risk of harm for individuals. Specifically, this broad approach raises concerns in several respects.

Firstly, the extension to “any other person” as a relevant reference point to determine whether an individual is identifiable means that any information relating to a data subject will be covered. As such, even anonymised data would have to be considered personal data as theoretically there may always be somebody who may have additional knowledge allowing for de-anonymisation, even if this is only the data subject who has encrypted its data. As there will be no secure way to anonymise data any longer, this effectively removes any incentive for privacy-enhancing measures such as encryption or hashing. Consequently, this broad approach to personal data runs counter the intended objective of the Regulation, effectively reducing individuals’ privacy protection, rather than increasing it, as companies might abstain from using or investing into privacy-friendly measures which are encouraged under Article 23 on data protection by design and by default.

This downside of the broad definition of personal data also becomes apparent in the context of consent. If every piece of information was to be considered personal data, then data subjects would continuously be confronted with extensive consent requirements and lengthy privacy policies. In consequence, granting consent would become an automatic reflex as hardly any service could be provided without the data subject dealing with data protection issues. The line between relevant and irrelevant aspects of data protection issues would become increasingly blurred, thus rendering the whole concept ineffective.

Secondly, the fact that Article 4(1) enumerates factors such as identification numbers, location data, online identifiers etc. as examples of personal data, suggests that these are deemed per se as relating to a data subject, thus qualifying automatically as personal data. By contrast, Recital 24 rightly clarifies that identification numbers, location data, online identifiers etc. cannot categorically be considered as personal data rather that it is dependent on the circumstances whether an individual can be identified on the basis of such factors, and where it cannot, these should not be considered personal data. We concur with this clarification as it recognises the inherent nature of such identifiers. For example, while website operators are generally not able to identify a person on the basis of the IP address, ISPs usually are. Similarly, if IP addresses are processed in combination with other personal data for certain purposes (anti-money laundering for example), they may be collected in an isolated fashion for advertising purposes. If all identifiers were to be qualified automatically as personal data, this would likely lead to a situation where a multitude of harmless processing operations would be subject to the requirements of the Regulation, causing additional administrative burden for businesses and supervisory authorities with no additional benefit for data subjects.

We urge EU decision-makers to abstain from such a broad ‘one-size-fits-all’ approach. Instead, the focus should be placed on the context and risk of processing to ensure that only those processing operations are captured, when there is a realistic risk of identification, and which involve a risk of harm to individuals. We suggest deleting reference to ‘any other person’ and clarifying that data will be considered personal if it is reasonably likely, given the context of processing, the means available to the controller as well as his intention to identify an individual, and that the controller is able to use the information for personal identification purposes. If there is only a remote, highly theoretical risk of identification, particularly because appropriate technical and organisational measures have been taken to minimise the risk of identification, then such data should not be treated as 'personal data'. Further criteria to be taken into consideration are the degree of risk of harm to individuals and the likely extent of that harm. More sensitive situations, with greater risk of harm and/or greater impact of this harm, would require greater precautionary measures in relation to the data than less sensitive ones. The introduction of such combined criteria, i.e. a subjective intentionality criteria coupled with the objective element of the context of processing, will allow focus on the really relevant data processing operations and will incentivise businesses to continue investing in privacy-friendly techniques and procedures. Furthermore, we believe that further clarification is needed regarding the status of anonymised, pseunonymised and encrypted data as non-personal data, particularly where appropriate industry standards and best practices or

recognised certifications are used to secure data. At a minimum, the ideas reflected in recitals 23 and 24 that the context is a relevant factor and that anonymised data is not personal data, should be expressly reflected in Article 4.

Fedil's recommendation:

Limit the scope of "personal data" by deleting reference to "by any other natural or legal person" from the definition and by introducing a reference to the context of the data processing, the risk of identification and the risk of harm for individuals. Amend Article 4 to reflect that anonymized and pseudonymized data are not to be considered personal data.

3. Consent requirement

Consent is one out of six legal grounds for processing personal data. Fedil considers that this important principle needs to be implemented in ways that are both appropriate for data subjects and companies and do not unnecessarily disrupt the use of a service. However, the current text proposed in the draft Regulation heightens consent requirements and introduces additional burden and more ambiguity.

More specifically and taking account of the specificities of online businesses, we consider that the requirement for consent to always be "explicit", irrespective of the context for which consent is being obtained or the risks involved in the processing operation for data subjects, is too formalistic and rigid, creating practical problems in the off-and online environment without adding anything to users' data protection. We take the view that the "explicit" consent requirement should instead be replaced by a context-based approach, which has the benefit of being more flexible as it takes into account the content and risks of a specific data processing operation. In light of the notion of an informed consumer we also deem it more relevant to focus on transparency with respect to the usage of personal data. A formalistic check-box approach would generally only result in an automatic reflex by the consumer, which ultimately does not lead to an increase in awareness, rather to the contrary.

Consent can in fact be inferred or implied from the action of requesting a service. For example, this is the case when a mobile user gives consent for being geo-located when requesting restaurant recommendations nearby. Yet, even if such action or behaviour is clear, it may not meet the threshold of "explicit" consent insofar as consent which is implied from behaviour is by definition "implicit": if we consider the situation of requesting a service based on geo-location data, the user's consent for processing such data is informed and implicitly given at the time of the request. The insistence on explicit consent for such a broad range of situations is also likely to lead to a "trivialisation" of the experience for data subjects. If they are asked to take affirmative action too frequently, they are likely to have trouble differentiating between the relative importance of different situations. The best way to guarantee meaningful consent is therefore in our opinion to allow for context-based consent.

Fedil would also like to question the notion of "significant imbalance" between data subject and controller in the context of consent (Article 7(4)) as it leads to significant legal uncertainty. We consider that the language proposed by the Commission is too broad and could actually miss its target. There is the risk that the utility of consent will be significantly restricted, as there is rarely an equal bargaining power between individuals and businesses. For instance, one could claim that there is significant imbalance where an individual relies upon the usage of a service for his business, therefore leading to some kind of dependency to this relationship. It would be excessive

to qualify such common examples as imbalanced and prevent usage of consent as a legal ground for processing personal data. As there are too many situations where one could claim an imbalance between the data subject and the controller, we believe this objective is better addressed on a case-by-case basis through the requirement that consent shall only be valid if it is "freely given", in the definition of consent (Article 4(8)).

Fedil's recommendation:

1. Guarantee meaningful consent by replacing 'explicit' consent requirement by a "context based approach" which takes into account the content and risks of a specific data processing operation.
2. Delete Article 7(4) which forbids the use of consent as a legal ground for processing personal data in case of 'significant imbalance' between data subject and controller.

4. Introduction of a new set of rights for data subjects

Fedil supports the idea that in order to guarantee trust and security in the Digital Single Market and to take into account new technological trends, the current set of data protection rules needs to be modernised. This should be done in a way that can be easily implemented by companies, that is technologically neutral and that does not create unnecessary obstacles for future innovation in the EU to the benefit of citizens.

In that respect, we would like to comment briefly on some of the key changes proposed by the Commission.

a. Right to be forgotten

While Fedil is generally supportive of a right to be forgotten as such, we believe a certain number of safeguards should be put in place in order to make it meaningful for users, workable for data controllers and enforceable by supervisory authorities.

We understand the term has been designed primarily for users of online services, particularly social network services. We do not want to put into question the relevance of a general deletion right in the "offline" world if such an obligation is compatible with other EU or national legislative instruments that companies have to comply with.

The Regulation should however not create false expectations for European citizens by making them believe that there are no risks involved in sharing or publishing information about themselves, as they can always revert to the right to be forgotten mechanism at a later stage. This may eventually prove counter-productive for the protection of data subjects considering that deletion of information published on the web is not always technically feasible. In addition, we believe that this right should not be designed as an absolute right given that other legitimate interests are often at stake which must be balanced with the right to be forgotten. Data controllers may indeed have many perfectly legitimate reasons "not to forget" users' personal data, including for fraud detection, anti-money laundering purposes or other legal retention obligations. Many regulatory and best practice requirements compel preservation of records. As an example, banks are required to retain identification documents (which include, amongst others, the customer's surname and first name, date of birth, full address, profession and reference number and date of the official identity document) for a period of at least five years beginning at the end of the business relationship with

the customer[3]. We therefore welcome the safeguards listed in Article 17(3) and (4), which rightfully limit the scope of its application to data that are not required to be retained by controllers for compliance purposes. However, we suggest clarifying the scope of the right to be forgotten by specifying that the controller's obligation to "forget":

- applies only where "forgetting" is technically feasible and does not involve disproportionate efforts from the controller;
- is technology neutral and may be complied with by appropriate means and protection techniques equalling deletion (e.g. rendering data anonymous or otherwise unusable, unreadable, indecipherable).

We appreciate the precautions surrounding the application of the right to be forgotten. However, in addition to the above, we are concerned by the requirement for controllers to take all reasonable steps to inform third parties about the request to erase any links to, copies or replications of the data. Article 17(2) does not seem to take account of the nature of the Internet and the ICT sector in general. When operating online, our member companies do not grant any kind of formal authorisation to third parties to publish information that has been made public on their website; once it is publicly available, they do not have any control on how this data are treated by third parties (they may be transferred, duplicated etc.). For the great majority of online services, this requirement would mean that controllers would have to look for every potential copy of any data that has been published on its website, which would practically amount to an obligation to police the Internet. Eventually, there are no obligations whatsoever for third parties that have been informed of the data subject's request to be forgotten to take any action for deleting his/her data. Article 17(2) does not bring any meaningful value to the right to be forgotten, on the contrary, the lack of clarity may lead to enforcement discrepancies, difference in the way users are treated from one platform to another and of course to a high degree of legal uncertainty for companies trying to translate this into practice.

Fedil's recommendation:

1. Clarify in Article 17(1) that the controller's obligation to "forget" only applies where this is technically feasible and does not involve disproportionate efforts, and may be complied with by appropriate means and protection techniques with equivalent effect to deletion.
2. Delete Article 17(2). At a minimum, it should be clarified that this requirement only applies when the controller has proactively made the data available to third parties, with which he has a contractual relationship.

b. Right to data portability

Article 18 of the proposed Regulation requires controllers to make data portable so that it can be transmitted from one controller to another "without hindrance from the controller from whom the personal data are withdrawn" (Article 18(2)). Fedil supports the rationale underlying the portability provision, which is to give individuals' control over their data. However, we are concerned that due to its wide scope and in particular the requirement to make the data transferrable, this provision may have detrimental effects to both data subjects and data controllers.

[3]Directive 2005/60/CE on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Firstly, we believe that data which has to be retained by the controller for compliance reasons should be excluded from the scope of the portability provision. Article 18 does not foresee any safeguards limiting the right to request transmission of such data to another service. Article 18(2) even explicitly mentions that the personal data must be "withdrawn" from the initial controller. We take the view that Article 18 should include a paragraph limiting the applicability of the right to data portability in situations where the data concerned must be retained for compliance reasons with a legal obligation by EU or Member State law to which the controller is subject.

Secondly, while we appreciate the Commission's intention to allow users to switch from one service to another as easily as possible, we take the view that data protection legislation is the wrong place to address such an issue. More important, imposing standards for electronic format, modalities and procedures for the transmission of personal data through EU legislation would both hinder competition and innovation in the online industry, which develops and uses many different kinds of mechanisms and formats for data export. Fedil acting as a multi-sector business association also wonders what would be the impact of these provisions on offline companies.

Finally, imposing the right to data portability for any type of personal data risks killing any incentive for economic operators to create new algorithms and offer innovative services to their users. The end result would be a homogeneous landscape of services combined with a decrease in research and innovation, hence less functionality and service quality, thereby frustrating user experience. Our proposed solution would be to differentiate between user-generated data that are uploaded by data subjects themselves (such as name, date of birth, email address and so on), and data that are the result of their interaction with the service providers. Such information carries significant commercial value and is being created by algorithms that are proprietary assets of the data controller. If this was perfectly transferable on a standard basis, there would be a risk that service providers would lose important competitive leverage.

Fedil's recommendation:

1. Clarify that the scope of Article 18(1) does not cover situations where data has to be kept by data controllers for compliance purposes.
2. Delete Article 18(2). At a minimum, restrict the scope of Article 18(2) to user-generated data only.
3. Refrain from imposing standards for data transmission by deleting reference to 'electronic format which is commonly used'.

c. Profiling

We appreciate the Commission's proposal regarding profiling as expressed in Article 20 of the draft Regulation and understand this to be the regulatory response to recent debates and concerns generated by the increased use of profiling techniques, particularly in the online environment. However, we would caution against the attempt to entrench an overly negative perception of profiling by means of special regulatory treatment of all forms of profiling irrespective of the objectives pursued. Naturally, as with any business process, automated profiles can be used to achieve aims that are undesirable and that may not be in the interest of consumers. However, the proposal seems to neglect the fact that there are many positive uses of profiling, which are actually welcomed by users. The aim of most profiling techniques is in fact for businesses to better understand customers' needs and provide them with better products and services. Profiling is therefore an important aspect of a competitive online marketplace. For instance, profiles are frequently used to satisfy consumer demand for technologies and services that remember their preferences, such as their native language or home country. Profiling is often the basis for a

customised shopping experience on online platforms, which is specifically tailored to the interests and needs of customers. It also helps to improve the services rendered to customers by online platforms. Furthermore, profiling is often part of a risk assessment process in certain industries, for instance to assess solvency/credit-worthiness of customers by online traders and financial institutions or to detect and prevent fraudulent behaviour in electronic payment systems. Profiling is an important tool to guide consumer behaviour as regards to energy efficiency and energy savings and hence contribute to achieve environmental goals, for instance through smart metering and smart grids.

We fear that Article 20, as currently drafted, will subject a number of legitimate practices with little privacy impact to overly strict obligations, for which there is no real need given the many safeguards that are already contained in the draft Regulation.

Consequently, rather than discouraging the use of profiling mechanisms as such, the focus of rules regulating profiling should be based on the purposes for which profiles are used and the degree of impact/consequence for the individual of such purpose. The Regulation should be amended to clarify that the controller's legitimate interest can provide a valid legal basis for the use of profiling techniques, particularly where it concerns fraud prevention, security purposes etc. Profiling should also be acceptable for beneficial purposes such as providing personalised and customised Internet experiences to users, while the strict requirements of the profiling provision should be reserved particularly to special categories of data (i.e. sensitive data). Such clarification would satisfy the need for legal clarity and consistency, ensure that the Regulation lives up to its objective of providing technologically neutral data protection, and strike an appropriate balance between protecting the rights of individuals and safeguarding innovation and commerce.

Fedil's recommendation:

Clarify that the controller's legitimate interest can provide a valid legal basis for the use of profiling and limit strict requirements of the profiling provision to special categories of sensitive data.

5. Data breach notification obligations

Data breaches and cybercrime are growing challenges for society. In that respect, a system that allows DPAs to be better informed about breaches is a key element in protecting personal information.

The proposed Regulation introduces new provisions on data breach notifications. All industry sectors are obliged to notify all data breaches to the DPA without undue delay and, where feasible, no later than 24 hours after having become aware of the breach. Controllers must also notify data subject where the breach is likely to adversely affect the protection of their personal data or privacy.

Fedil is concerned that the current wording may lead to over-notification to DPAs and will overall prevent effective implementation of rules by controllers and DPAs alike.

A mandatory notification requirement to DPAs for all breaches, even minor ones, will significantly increase the number of notifications as controllers will report every breach. The 24-hour deadline is problematic as it does not provide sufficient time to fully assess the nature of the breach, its impact as well as the most appropriate solution to tackle the effects of the breach. There is a risk that the

provision as proposed will impose significant compliance burdens not only on controllers but also on DPAs and trigger "notification fatigue" amongst consumers.

The aim of data breach notification rules should be to promote best practices in raising data subjects' awareness about a breach, providing them assurance that their personal data is handled in a secure and safe fashion and to propose appropriate solutions. A workable system should therefore be based on a threshold that is itself based on the concept of "significant risk of serious harm" for the notification to data subjects and hence oblige companies to notify breaches to DPAs in a reasonable delay instead of a 24 hours' notice (thereby ensuring consistency with the breach notification requirement stipulated in the e-Privacy Directive). The notification obligation should only apply in limited cases, e.g., where disclosure concerns sensitive data, data covered by a professional secrecy or where a significant number of data subjects are concerned. Furthermore, breach notification rules should allow for an exemption to notify breaches when technical protection measures have been implemented to render the data unintelligible. We believe that such a system, as it is currently in effect in e.g. Germany, leads to a more risk-adequate balance.

Fedil's recommendation:

Introduce a workable system for data breach notification based on a threshold that is itself based on the concept of "significant risk of serious harm" and that obliges companies to notify breaches to DPAs in a reasonable delay. Delete reference to the 24 hour notice deadline.

6. Administrative obligations for controller and processor

Fedil considers that the accountability principle is a very useful concept that can have a positive impact on companies' behaviour as it encourages controllers and processors to put consumers' privacy high up on the agenda, be responsible and accountable with respect to existing privacy risks and put in place policies and processes to mitigate those risks. Accountability can be effectively implemented by taking an ex ante rather than an ex post control approach, thereby reducing the burden on businesses and DPAs, and by granting benefits to companies demonstrating a responsible approach to privacy, which will incentivise the use of privacy enhancing measures ("Privacy by design").

However, we are not convinced by the manner the accountability principle has been incorporated into the Regulation. Indeed, Fedil regrets to see that the Commission proposal is very prescriptive and lacks flexibility. Instead of encouraging the use of privacy enhancing measures, thereby reducing the administrative obligations on controllers and processors, it introduces new and onerous requirements that will substantially increase disproportionate administrative burden for businesses without any regard to the potential privacy risks.

This concerns in particular controller obligations regarding:

a. Documentation, privacy impact assessments and prior consultations and authorisations

The proposed Regulation replaces the current obligation to notify all processing operations to the DPA with a requirement for detailed documentation as well as requirements to conduct privacy impact assessments and obtain prior clearance from DPAs, thereby creating a system that is

significantly more burdensome for both controllers and processors than the initial notification requirement.

The proposed documentation obligations are very detailed and the Commission is mandated to lay down standard forms for the documentation. We stress that data processing can be documented well in many ways and no specific method should be mandated. The obligation is disproportionate since it covers almost all processes. Documenting will be a very extensive process, especially when joint responsibility is introduced. The obligation will trigger high costs, also for low-risk processes. Therefore, Fedil asks for the introduction of exceptions for low-risk processes, as they may be encountered in many business sectors and activities.

Furthermore, prescriptive provisions on privacy impact assessments risk create a rigid approach to data protection without any consideration of the risk associated. The proposed provisions on privacy impact assessments and prior consultations increase the administrative burden on businesses and supervisory authorities alike but also on consumers without reflecting the good practice of planning and assessment work done by companies. There should be no prior consultation obligation for data processing, which according to the assessment is in compliance with data protection legislation. Also the obligation to consult data subjects or their representatives should be deleted as it could e.g. risk the confidentiality of information and trade secrets.

b. Data protection officers

The proposed Regulation introduces an obligation for controllers and processors to designate a data protection officer (DPO) for companies employing more than 250 persons or where the core activities of the controller consist of processing requiring regular and systematic monitoring of data subjects.

While Fedil recognises that compliance with data protection rules is of utmost importance, these prescriptive and detailed provisions will be costly and burdensome, in particular for organisations (online and offline) where data processing forms only a marginal part of their activities,

In order to limit the cost of compliance and the administrative burden on companies, the appointment of a DPO could be linked with the benefit of an exemption from detailed documentation, impact assessment and pre-clearance requirements. An incentive for accountable controllers could also be a simplified system for international data transfer.

Fedil's recommendation:

Achieve a more efficient approach by balancing administrative obligations and companies' accountability, encouraging the use of "privacy enhancing measures" instead of introducing prescriptive new administrative measures.

7. International data transfers

We appreciate that, in recognition of the international dimension of many businesses, the proposal contains a number of key improvements that are aimed at making international data transfers easier for companies. These are essential elements in positioning Europe in a globalised economy based on a growing number of data exchanges. In that regard, Fedil welcomes the formal recognition of

Binding Corporate Rules (BCR) in the proposed Regulation as a means for complying with data protection rules in international data transfers within organisations.

Nonetheless, Fedil members feel that the new rules as proposed are a missed opportunity. Data transfers are still, except in the case of BCRs and standard contractual clauses, subject to prior authorisation from the lead DPA. A notification system would have been a much more efficient way to regulate data transfers by still providing appropriate safeguards for data subjects.

Moreover, we believe that it is necessary to revise and further simplify the regime of standard contractual clauses, which are an important instrument particularly in the context of cloud computing, where international data transfers occur on a regular basis. Where contractual clauses have been approved by the lead DPA in accordance with Article 42.2(d) no further authorisation from the DPA should be required, if the approved clauses are used by the controller as "model clauses" for further data transfers to other processors or recipients. Furthermore, we deplore that standard contractual clauses as currently designed in Commission decision 2010/87/EU can only be used in constellations when an EU-based cloud customer/user (i.e. the controller) makes use of processors (i.e. cloud providers) that are based outside of the EU, whereas these cannot be relied upon when a European cloud provider (i.e. processor), as the data exporter, wishes to enlist a sub-contractor who is based outside of the EU (for instance in order to make use of their storage capacity). In addition, agreements which are based on those standard contractual clauses are only effective if directly signed by the controller and the processor established in the third country. This does not take account situations where there is more than one provider involved in the delivery of cloud solutions. In fact, in today's reality, a growing number of cloud solutions made available by cloud service providers are bundled products of services delivered by multiple, globally located independent vendors of service solutions. This ever-increasing globalisation of product delivery processes requires an adaptation of the legal framework for standard contractual clauses allowing for a "sub-contractor" regime that also applies to the export of personal data in third countries without the direct involvement/consent of the controller.

In addition, we believe that international data transfers could be further facilitated by means of the data protection officer, an instrument that has been introduced in the draft Regulation as a mandatory requirement for larger companies with a view to reinforce accountability of those processing personal data. We believe that companies, who live up to these enhanced accountability requirements by nominating a data protection officer, should be rewarded by relieving them from any further administrative requirements for data transfers. For instance, they should be allowed to transfer data without any further authorisation from or notification to the lead DPA.

Considering all the strict safeguards that the draft Regulation imposes on controllers, notably in terms of accountability, we believe that a more self-regulatory system for data transfers to non-EU/EEA or assimilated countries would be justified and appropriate. It is our firm belief that data protection goals are best served if adequate data security measures are in place in order to technically prevent most, if not all of the risks that texts and contracts also seek to avoid.

Fedil's recommendation:

Further simplify administrative constraints on international data transfers through better use of instruments such as the regime of standard contractual clauses or a more self-regulatory system for companies who have reinforced their accountability.

8. Cloud computing – Definition, responsibility and liability

Data protection is one of the main reasons why many companies are hesitant to make use of cloud services. The uptake of new technologies such as cloud computing in Europe will therefore depend very much on whether the new EU Data Protection Framework is sufficiently clear, workable in practice and designed to accommodate the realities of the cloud business environment. For the development of cloud services and the promotion of new cloud business models, it is crucial that actors operating in the cloud know if and to what extent they are subject to EU data protection obligations, how responsibilities and liabilities in terms of privacy protection are to be allocated between them and that the burden placed on the different parties is appropriate to their respective roles in the business ecosystem.

We take the view that the proposed Data Protection Regulation, particularly the rules relating to the controller/processor concept and the respective distribution of responsibilities and liabilities, structurally do not cater for many types of cloud computing services and we are therefore concerned that it will impede rather than promote their further development in Europe.

a. Controller/processor concept

The draft Regulation maintains the traditional controller/processor concept, defining a controller as the entity which determines the purposes, conditions and means of processing of personal data, while the processor is understood to be the entity that processes personal data on behalf of the controller. This concept is critical as it determines the obligations and liabilities in terms of data protection compliance. The status of a cloud service provider (CSP) as controller or processor will depend on the context and the nature of his relation with data subjects. However, as a general rule, CSPs tend to be commonly characterized as processors, while cloud customers/users are usually qualified as controllers.

Considering today's sophisticated cloud environment with many different business models, multiple actors and layered arrangements between providers, this static categorisation is unsuitable and therefore very difficult to apply in practice. In fact, a number of CSPs should not even be qualified as processors given that their services are fundamentally different to those of a standard processor. Indeed, depending on the nature of the service offering, CSPs host and give access to infrastructure facilities (IaaS), such as processing power, storage, networking equipment and other basic computing resources, to software development tools for the creation and deployment of customised applications (PaaS), or to software solutions (SaaS), which are used by the cloud customer/user for purposes that are usually unknown to the CSP. The processing of data happens in a fully automated way, within the limits of the offered cloud solution and under the sole and full control of the cloud customer/user, as most cloud solutions are delivered with the required management tools.

Unlike traditional processors who access and manage data for the controllers, CSPs are ultimately data-agnostic. Their view on the data is restricted to an absolute minimum and usually their access possibilities are strictly limited to the system data in order to be able to manage the user accounts and provide a proper support service. For example, a provider of an online web hosting solution manages and bills the subscriptions of his customers. He does not supervise the type of user content uploaded and published on the website. Particularly IaaS providers regularly do not know whether information stored on or processed through their infrastructure is "personal data" and they usually have no control over or ability to access that data, nor do they require such knowledge or access to provide their services. This is also obvious with respect to the emerging cloud broker business, where cloud service brokers are just reselling access rights without being involved in the

hosting and/or management of the cloud solution they give access to. Furthermore, a growing number of cloud solutions include encryption tools that encrypt the user content even before being submitted to the CSP or feature other appropriate technical and organisational measures in order to prevent access to the data by anyone other than the cloud customer/user. In these situations, nobody besides the cloud customer/user himself can process, access or even display his content. Hence, assuming that the CSP is always directly involved in the processing and has access to or even has a view on the data processed via the cloud solution he is providing, is not reflecting the realities of today's cloud industry.

The examples listed above show that CSPs, particularly where they do not have knowledge as to the nature of the data on their infrastructure and/or do not have the practical ability to access such data, cannot reasonably be considered as processor. They should rather be qualified as neutral intermediaries, unless the CSP takes measures to accessing or using the personal data in breach with its contractual obligations or in excess of its authority in relation to that data (in which case it is justified to consider such provider a controller who should be liable as such).

We therefore suggest revision of the definitions of 'controller' and 'processor' so as to allow for a more nuanced and balanced approach with a view to accommodate the specificities of new technologies and business models. The draft regulation should provide for different actors with varying degrees of obligations and liabilities under the data protection law.

b. Allocation of responsibilities and liabilities between controller and processor

EU data protection law has so far always been governed by the basic principle that the controller has primary responsibility for complying with legal privacy obligations and faces primary liability for any data protection law breaches. The controller may use another entity to process personal data on his behalf. However, he remains the exclusive point of contact for data issue related claims and vis-à-vis DPAs. Conversely, with a view to enable the controller to comply with his privacy obligations, the processor is required to act on the controller's instructions only and the controller's obligations need to be laid down in a written controller-processor contract. Processors are not normally directly subject to the data protection regulatory framework; their responsibilities and liability is strictly limited to what has been contractually agreed with the controller.

While the draft Regulation continues to place the onus for compliance primarily on the controller, it considerably extends the responsibilities of data processors (see Articles 24, 26, 27 and 28), thereby further blurring the initial distinction between controller and processor, ignoring the complex contractual set-up between these players and the limited access/control possibilities processors often have over the data they process. Newly introduced obligations for the processor are for instance the requirement to assist the controller in carrying out data protection impact assessments, to obtain prior authorization or to consult DPAs, and to maintain, in addition to the controller, detailed documentation of all processing operations. This increase in direct obligations imposed on processors is coupled with a new liability provision, whereby the processor is jointly and severally liable with the controller for damages, unless it can prove it is not responsible for the event giving rise to the damage.

We take the view that this extension of the processor's responsibilities and liability unnecessarily interferes in the contractual relationship between controller and processor, the aim of which is to ensure that processors undertake the required measures so that the controller can comply with his obligations. It further complicates the already complex relationship between controller and processor, leading to additional confusion and uncertainty and is even less compatible with new business models such as the cloud than the existing legal solutions. Many CSPs will not be in a position to comply with many of these additional obligations, because, as explained in previous paragraphs, they usually do not have access to the data or processing strategies, are not aware of

the nature of the data in their infrastructure, its importance to the cloud customer or the risks linked to it, and are hence unable to comply with detailed information requirements, conduct data impact assessments or make any determination as to the treatment of the personal data.

Furthermore, even if the CSP assists the controller at the moment of the service subscription, things might change over time, without the CSP being involved or being aware. This risk is greater when the cloud solution provides the option to store the user content outside of the hosting environment of the cloud solution. The user content only remains within the area of influence of the CSP for a very short period of time and can change from one login to the next. Any extension of the CSP's responsibilities regarding user content will expose him to unpredictable and unmanageable risks. As a result, CSPs will not be able to guarantee continual compliance with any regulation that allows the controller to transfer any kind of responsibility and accountability to the CSP.

In light of the above, Fedil would urge the EU legislator to revisit the controller/processor concept as well as the chosen allocation of responsibilities between them, and amend Articles 2.3, 4(5), 4(6) and Chapter IV of the draft Regulation accordingly. We suggest opting for a more flexible and nuanced approach, recognising that there may be different entities involved in the treatment of personal data and ensuring that each entity is only responsible and liable to the extent it has reasonable means of access to or control of the data. Providers, who do not have any knowledge as to the nature of the data they process or store on their network and/or who do not have any meaningful access to it, should not be classified as controller nor processor, but should rather be considered neutral intermediaries, and as such, they should benefit from the liability "defense" provisions as stipulated in Articles 12 to 15 of the E-Commerce Directive. For the rest, the parties should be free to allocate risks and responsibilities amongst them contractually.

Fedil's recommendation:

1. Revisit the controller/processor concept in Articles 4(5) and 4(6) and introduce other categories of actors with varying levels of responsibility and liability, in particular the category of 'neutral intermediary' for actors without any meaningful access to or control of data (with additional link to Article 2(3)).
2. Revisit the chosen allocation of responsibilities between controller and processor in Chapter IV. In particular, delete all reference to 'processor' in all provisions concerning the controller's obligations (Articles 28 – 34, 53, 75, 77 and corresponding recitals) and amend Article 26(2) to clarify that the obligations in this Article only apply where the processor is able to assist with reasonable effort and insofar as this is possible given the nature of processing.

Conclusion

As highlighted above, Fedil supports the approach chosen by the Commission to facilitate the free flow of information in the Internal Market, namely a fully harmonized single set of data protection rules applicable throughout the EU, coupled with a one-stop-shop enforcement mechanism. However, we urge EU legislators to revisit the rules on how to comply with general principles and consider providing for a true accountability-based approach that lives up to its name. Rather than being detailed and prescriptive, the Regulation should introduce real incentives for companies to act responsibly.

Fedil looks forward to working with the EU Institutions and Member States and to sharing our experience and expertise when it comes to the protection of personal data in the European Union and abroad. We would be happy to discuss these points and the broader revision of Directive 95/46/EC in more detail.

Luxembourg, 17th of July 2012

About Fedil-Business Federation www.fedil.lu

Founded in 1918, Fedil – Business Federation Luxembourg is today a multi-sector business federation representing the industry, construction and business services sectors among which the ICT industry. On a national level, Fedil's objectives are to protect the professional rights and interests of its members, and provide analysis on any related economic, social and legal questions arising. On a community level, Fedil is associated with the Confederation of European businesses BUSINESSEUROPE (www.businesseurope.eu), and has a representative office in Brussels.