EDiMA Position on the Proposal for a Regulation on the Protection of Personal Data in the EU

The European Digital Media Association (EDiMA)[1] welcomes the European Commission's proposal for a new Data Protection Regulation. The current review of the EU's Data Protection Framework provides an important opportunity to establish harmonised rules and principles aimed at strengthening individuals' privacy while also promoting the development of the Digital Single Market and innovation in the EU.

Striking the right balance will require an approach that ensures such new rules are adequately future-proof, and not so prescriptive as to hinder innovation or detract from the review's broader aims. Focus should be placed on a principles - and context - based approach that enhances individuals' privacy while also providing greater legal certainty for businesses.

Although its objectives are to be welcomed, EDiMA believes that the spirit of the proposed Regulation, poses significant challenges for online platforms operating in Europe and, in fact, could have counter-productive effects on individuals' protection(s) online. Accordingly, we encourage EU decision-makers to examine in detail the following key areas and corresponding EDiMA considerations and recommendations highlighted at greater length in the pages which follow:

1. Intermediary liability in the context of data protection
2. Definition of 'personal data'
3. 'Main establishment', jurisdiction & role of the 'lead DPA' and territorial scope
4. Consent
5. Right to be forgotten
6. Data portability
7. Accountability
8. Controller/processor responsibilities in the context of cloud computing
9. Delegated acts

EDiMA believes that further work and consideration is needed in these key areas in order to ensure a legal framework conducive to the development of the Internet economy and the protection of individuals' data online. We look forward to working with EU policymakers and stakeholders to achieve such objectives.

Intermediary liability in the context of data protection

We welcome the draft Regulation's reference to the applicability of the intermediary liability limitations of the E-Commerce Directive (2000/31/EC), which are horizontal in nature and therefore apply to all information society activities. The draft privacy and data protection Regulation determines what constitutes a privacy and data protection infringement, while the E-Commerce sets

[1] The European Digital Media Association (EDiMA), is an alliance of Internet platform companies whose members include Amazon EU, Apple, eBay, Expedia, Google, Microsoft, MIH Group, Nokia, Yahoo! Europe, Orange and others. EDiMA's members provide Internet and new media platforms offering users a wide range of online services, including the provision of audiovisual content, media, E-commerce, communications and information/search services. EDiMA represents Internet platform businesses in EU policy formation, on matters affecting the online environment and believes EU policy should maximise the development of new online services and business models to the benefit of innovators and EU consumers.

out the conditions by which an information service provider is liable for third party infringements of the law.

Intermediary liability protection is fundamental to the viability of the Internet as it exists today. Any platform that hosts user-generated content (including online social networks and certain cloud computing providers) relies on protection from intermediary liability for its commercial viability and even survival. The Regulation does not sit in isolation from other instruments of EU law and Recital 17 and Article 2(3) of the Commission proposal should absolutely be preserved.

Definition of 'personal data'

The **definition of** '**personal data**' is a fundamental concept prompting the application of the strict obligations and liabilities for controllers and processors. It is therefore vital that the definition provides sufficient legal clarity, adapts to different scenarios and realities and is future-proof.

The definition as currently proposed in Article 4(1) and (2) substantially extends the scope of data covered by the EU data protection rules by 1) reverting to the means of 'any other person' to determine whether an individual is identifiable in the definition itself; and 2) by qualifying factors such as identification numbers, location data, online identifiers, etc. as being per se personal data.

The new definition applies the identifiability test of a 'data subject' to an unlimited data set beyond the knowledge of any data controller. It follows that every 'person' is a 'data subject', regardless of the data controller's ability to identify them, and therefore that all data relating to any person at all must be considered personal data per se. In other words, the definition does away with the distinction between a 'person' and a 'data subject'. As a result, companies are forced to presume that any data they hold is personal.

This all-encompassing approach will effectively result in the strict conditions of the Regulation applying to the vast majority of all processing operations, regardless of the context in which the data is processed, whether the data at hand is attributable to a person, and the realistic risk and intention of identification. It also risks removing any incentive for companies to invest in or make use of privacy-enhancing measures and processes, such as anonymization and pseudonymization techniques (encryption, hashing, etc.) as under such an approach any piece of information, even if anonymized, would have to be considered personal. As a result, the broad definition of personal data risks leading to a reduction, rather than an increase, of individuals' privacy protection, which would of course directly conflict with the intended objective of the Regulation.

Example 1 – Internet Protocol (IP) addresses: When a user accesses a website via his device, his IP address will automatically be sent to the server of the website so that the server knows where to send the internet page, and possibly also to third parties for them to show their content to the user on this website. In all these cases, the user's IP address is usually processed by the server of the website operator and the third party in anonymized fashion (e.g. truncated) for the purpose of the user's protection and security. Neither the website operator nor the third party is usually able to identify the user simply on the basis of the IP address. Only the Internet Service Provider (ISP) of the user is able to relate an IP address to a user's identity. Due to the broad definition, IP addresses would per se qualify as personal data under any circumstance, despite (1) the fact that the website cannot identify the user on the basis of its proper means, (2) the fact that the website operator/third party does not need or intend to identify the user for the processing purposes and (3) the lack of risk for a user's privacy involved in the processing of IP addresses. Consequently, companies may refrain from rendering IP addresses anonymous given that the strict requirements of the Regulation will apply in any case.

Example 2 – Cloud computing: Cloud service providers usually recommend to their customers to encrypt their data before uploading it to the cloud network. Encrypted data is not accessible to the cloud service provider as it does not have the key to read the data. Hence, it cannot link this data to any individual, and would not even be in a position to determine whether this data is personal or not. Nevertheless, in application of the broad personal data definition even anonymized data, such as encrypted information, would have to be considered personal data as theoretically there may always be somebody (i.e. 'any other person') with relevant knowledge allowing for de-anonymization, even if this is only the cloud customer/data subject who has encrypted his/her data.

Example 3 - Identification numbers: Mobile phone manufacturers maintain databases listing identification numbers of devices (IMEI) to document that they have produced devices with numbers officially allocated to them (by the GSM Association). This data is in no way connected to the (future) users of the devices. However, due to the broad personal data definition, in particular its reference to 'any other person', one could argue that for instance a mobile network operator is theoretically able to draw a link between the database and the device user. While such serial numbers combined with customer information in the hands of network operators are personal data, it would not make sense to also qualify the manufacturer's data bases as personal data and to apply the rules of the Regulation to them. Other similar examples include telephone numbering spaces allocated to countries or regions by the International Telecommunication Union (ITU) or IP addresses allocated to ISPs by the Internet Assigned Number Authority (IANA) which are not linked to data subjects.

Example 4 - Web analytics: Analytics providers provide essential services by collecting data from a very large array of sites and aggregating it. The statistics that can be generated from such data aggregation can be used for a wide range of purposes such as optimization of website elements, website performance measurement and analysis, and adserver analytics for billing purposes. Indeed, accurately measuring user interaction with online ads is structurally mission-critical for the online advertising industry. While the aggregate data generated by analytics services may be derived from data that could be considered personal under the new, broader definition, it is not intended to result in user profiles or targeting of any ads or content to specific users, but rather as large-scale management information. It can be processed using privacy-protecting pseudonymization techniques, but the draft Regulation lacks sufficient incentives for providers to do this because all 'personal data' that is not sensitive is treated equally.

The fact that Article 4(1) of the Regulation lists identification numbers, location data, online identifiers, etc. as examples of personal data, thereby implying that these are considered to relate *per se* to a data subject, complicates the situation even further. It also contradicts with Recital 24, which rightly clarifies that such information cannot categorically be considered as personal data; rather, that it depends on whether an individual can be identified on the basis of such factors and, where it cannot, these should not be considered personal data.

The negative impact of such a broad definition is also illustrated in the **context of consent**. If every piece of information is considered personal data, users would continuously be presented with extensive consent requirements, impacting the customer experience without adding anything to the user's protection. Providing or indicating consent would become more reflexive, or automatic, given that many, if not all, online operators rely on consent as legal basis for a number of processing operations to be able to provide their services.

Rather than instituting such an all-encompassing approach to the definition of personal data that would likely run counter to the aims of the Regulation, EDiMA would suggest clarifying the scope of Article 4(1) by:

- Deleting the reference to 'any other natural or legal person' as well as to factors such as location data and online identifiers;

- Inserting language in Article 4(1) and corresponding recitals clarifying that the context of the specific processing operation is decisive to determine whether an individual is identifiable, which should cover aspects such as the means reasonably likely to be used by the controller in its regular course of business to identify an individual, the effort required, the technical feasibility and the purposes/intentions pursued by the controller. Account should also be taken of any technical and/or organizational measures that the controller has put in place in order to prevent identifiability. If the controller is able and intends to use the information to identify the data subject, such information should be qualified as 'personal data'. If such possibility is only remote and primarily theoretical, it should not be treated as 'personal data'.
- Clarifying the term 'anonymous data' and expressly stipulating in Article 4(1) that information which has been rendered anonymous in such a way that it can no longer be attributed to a data subject, including where any personally identifying features are replaced with a code so that the data subject is no longer identifiable, or that such attribution would require a disproportionate amount of time, cost and effort, does not qualify as personal data and should therefore fall outside of the scope of the data protection rules.
- Introducing language recognizing the value of pseudonymous data and subjecting the processing of such data, which shall be considered personal data, to more lenient requirements (e.g. processing of such data shall be considered lawful in accordance with Article 6 and data subjects shall have the right to object to the processing of such data in accordance with Article 19). Pseudonymous data should be understood as personal data that has been collected, altered or otherwise processed in such a way that the data subject's name and other identifying features are replaced with another identifier so that identifiability of the data subject is considerably impeded.

EDiMA is convinced that such an approach will result in enhanced protection of individuals' data given the warranted emphasis on the most relevant data processing operations and the setting of true incentives for industry to continuously invest in privacy-friendly technologies.

'Main establishment', jurisdiction & role of the 'lead DPA' and territorial scope

EDiMA welcomes the introduction of a 'one-stop-shop' approach with respect to the jurisdiction of Data Protection Authorities (DPAs), as it has the potential to help simplifying the administrative hurdles linked to data processing and ensuring a consistent and more efficient application of data protection rules across Europe.

Clarity with respect to the competent regulator is particularly crucial for businesses operating in several Member States, as they require legal certainty as to one 'lead' regulator being their single point of contact and by whom they may be addressed, and it is also essential to allow businesses and consumers to fully reap the benefits of the EU Single Market. The current system has led to confusion as to competency questions and to conflicting approaches by regulators as a result of this.

In order to achieve a true one-stop-shop and avoid confusion over the determination and role of the 'lead DPA', we think that the concept of 'main establishment', the decisive factor for such a determination, as well as the role of the 'lead DPA' requires further clarification.

The set of criteria in the current draft which determines the 'main establishment' (Recital 27 and Article 4(13)) is too narrow to work in different situations and provides too much room for diverging interpretation. The main reference point for controllers, i.e. the place where management activities are exercised determining the main processing decisions, is too vague to allow particularly groups of companies with several establishments in the EU to clearly determine the degree of autonomy their

entities can have and hence which of their entities is the 'main establishment'. It may therefore lead to situations where several DPAs claim jurisdiction over group entities. In addition, the fact that a different test applies to processors (decisive factor being its place of central administration) further complicates the situation, particularly where businesses are controller and processor at the same time for different processing operations.

To take account of today's business reality and provide for clear-cut and common sense criteria allowing for flexibility and predictability for all stakeholders, we take the view that the Regulation should provide for the following:

- A single uniform 'main establishment' test, applicable to 'undertakings/groups of undertakings', whether controller or processor, as the relevant reference point, and based on a set of relevant objective criteria, which a business can choose from in order to officially designate its location of 'main establishment';
- Such set of criteria should include the location of: a group's European headquarters, the entity within the group with data protection responsibilities, the entity which is best placed (in terms of management, administrative functions etc.) to deal with and enforce data protection matters, or the entity where most decisions in terms of processing are taken;
- The lead regulator should be informed of the official designation of the place of 'main establishment' and the associated determination of the lead regulator with binding effects for a specific period.
- Such designation should apply to all entities part of the group established in the EU and the 'lead' regulator should be competent to supervise all processing carried out by all entities of the group as far as they are subject to the Regulation.

A similar concept has been developed 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 the very same objective criteria. 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' in the context of the draft Regulation. We believe that such a transparent and consistent approach, which could be accompanied by a dispute resolution system amongst DPAs in accordance with the consistency mechanism as well as appeal possibilities for businesses, will provide for legal certainty required by business while preventing the risk of forum shopping as well as disputes over the place of main establishment.

Further, we believe that the role and function of the 'lead DPA', as well as the cooperation between the regulators as per the so-called consistency mechanism contained in Chapter VII of the draft Regulation, needs to be clarified so that it can effectively operate as a true 'one-stop-shop'. The role of the lead DPA as currently described seems to be limited to supervision, cooperation and coordination; its enforcement powers over businesses under its jurisdiction in cases with a cross-border dimension are not clear. The current wording of Chapter VII seems to suggest that any DPA can initiate enforcement action against companies which are not under its jurisdiction. This might affect the 'one-stop-shop' concept and ultimately lead to inconsistencies in the application of the Regulation. We would therefore suggest clarifying that the lead DPA has exclusive competence over companies that have their main establishment in its jurisdiction and that other regulators who receive a complaint or wish to launch investigations for other reasons should be required to refer such matters to the lead DPA, which should be obliged to cooperate.. This clarification will help to provide consumers and companies with legal certainty as to which competent regulator has authority to supervise any data processing activities subject to the Regulation and will prevent multiple regulators from sanctioning the same company for the same incident.

Finally, we consider that there is no reason why companies that are not established in the EU but that are subject to the Regulation, and that name a representative established in the territory of the Union, should not benefit from the one-stop-shop concept. While the right and obligations apply to non-EU companies when they offer goods or services to the EU and/or monitor the behaviour of individuals in the EU are equal to EU established companies, the former cannot benefit from one of the main anchors of the draft Regulation, namely the Digital Single Market and the one-stop-shop concept. This differential treatment needs to be removed as it risks being considered against the EU principle of non-discrimination.

Consent

Consent being an essential legal basis to process data, EDiMA believes that this concept needs to be implemented in ways that provide appropriate protection for individuals without unnecessarily disrupting the use of a service while being clear and workable for businesses.

However, the consent regime as proposed by the Commission could, as drafted, have a **dramatic effect** on today's Internet and mobile business models, while simultaneously doing little to increase users' protection. Four factors in the Commission's proposal contribute to this:

1. Due to the broad definition of personal data, a vast amount of information will be captured that can either often not be linked to an individual by a data controller or, if it can, will often be rendered anonymous or pseudonymous and, as a consequence, its processing can be considered harmless. Nevertheless, with a substantially broadened scope, consent will have to be provided substantially more often.

2. Consent must always be explicit and affirmative. The prescriptive 'one-size-fits-all' approach to all circumstances in the offline and online world fails to take into account the many different types of situations and contexts for which data is being collected, the purposes for which it is used, and the privacy risks involved. The expected overload of consent requests, even in trivial situations, is likely to confuse users, who will find it difficult to determine the situations that matter to them most. Individuals' privacy protection is likely to decrease as a result of such an approach. Moreover, there is currently a wide range of mechanisms that effectively enable users to control and consent to collection and use of their information depending on the circumstances involved. Mechanisms, for example, which provide complete information on how personal data will be used, can often be more protective of consumer privacy than others which may require explicit consent, but which do not offer as much context and complete information. By preferring one mechanism over others, the Regulation diminishes the incentives to develop different and potentially better privacy protecting solutions.

3. Putting the burden of proof on controllers to show they have received consent means that companies will have to keep a record of each and every consent event (e.g. clicks) from any given user; and, as a result, this may bring a disservice to, rather than protect, data subjects. With a view to minimizing disruption of the user experience and subjection of the user to 'consent fatigue', websites will likely move to a registration and authentication system as a condition for the use of a service. It seems contrary to the objectives of the Regulation to incentivise the collection of more information from users than is actually needed. It also seems inappropriate to create major incentives for the logged-in user business model over other models, particularly as this would likely lead to fundamental changes to the way the Internet is experienced today: competition with established global brand names for the trust of users will become increasingly difficult, significant industry consolidation can be expected and a resultant reduction in innovation.

4. Excluding consent in situations where there is 'significant imbalance' between data subject and controller means that consent cannot be relied on in many situations 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 on the usage of a service for his business.

We believe that the Commission has not chosen an effective way to strengthen the rules. Instead of taking such a prescriptive approach, the Regulation should allow innovators to use mechanisms to obtain consent that reflect how and in what contexts data will be used, without undermining customers' experience and expectations. We therefore suggest the following changes:

- Reference to explicit consent should be removed and replaced by a **context-based approach** so as to allow for flexibility, ensure that there is a role for implicit consent, in cases where a user's action can safely be interpreted as a decision to accept certain uses of data, and that explicit consent is reserved for decisions of significant importance; for instance, where sensitive data is at stake. Language should be inserted clarifying that the method used to obtain consent should be dependent on the context, i.e. the nature of the data to be collected and the processing purpose.
- The requirement of **burden of proof on controllers** to always prove consent **should be removed**.
- **The notion of 'significant imbalance' should be deleted** as this criterion is too vague to be workable in practice. Questions of imbalance should rather be assessed on a case-by-case basis via the existing requirement that consent shall only be valid if it is 'freely given'.

Right to be forgotten

We believe that the role of intermediaries, and in particular as regards the right to be forgotten, should be clarified in the direction that intermediaries cannot be made responsible or liable for the discovery or processing of information that is legal at source. In other words, if the publication is lawful, there should be no doubts about the lawfulness of its discovery and access. This fundamental principle cannot be put into question by trying to accommodate definitions of controller and processor to online intermediaries, as they do not exercise control over the information

We believe that the right to be forgotten and erasure constitute a repackaging of existing rights to object, accuracy, erasure and rectification. However, the obligations proposed with regards to third parties (Article 17.2) remain unclear and are not proportionate from the outset. In addition, the right to be forgotten has started to be interpreted differently in Member States, and it could lead to situations that surely could not be intended by the European Regulator.

EDiMA is concerned by the requirement for controllers to "*take all reasonable steps to inform third parties of 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. Visitors of our member companies' sites can freely copy, transfer and duplicate any information published, including personal information. This is part of the principle of openness of the Internet and the very essence of their services. They do not grant any kind of formal authorisation to third parties to publish that information; however, once it is publicly available, they do not have any control over the way in which such data are treated by third parties.

Similarly, the open nature of the Internet and the huge volume of information online also mean that search engines are not and cannot be in a position to check the truth, accuracy or justifiability of the information they index or process under the instructions of the user. Expecting search engines to restrict the discoverability of otherwise legal information is disproportionate and perfectly

inappropriate. It would clearly be unnecessary as the information would remain publicly available despite significant burdens imposed on search engines. Those burdens would undermine the ability of search engines to provide their services. Furthermore, restricting access via search engines would also undermine the ability of publishers to defend their rights, which include the dissemination and accessibility of the information they chose to publish. While the right to freedom of expression applying to journalistic purposes is recognized in the context of the right to be forgotten, we consider that the recognition of other angles of the fundamental rights to the freedom of expression and information need to better inform the language of these provisions.

Search engines and online intermediaries nevertheless serve an important public interest: in many cases the third-party publication that underlies a search result is an exercise of the right to freedom of expression or freedom of the press, while the user discovering content with the help of a search engine is exercising the fundamental right of freedom of information. Article 11 of the Charter of Fundamental Rights of the EU protects the freedom of expression and the freedom of information, including on communication networks such as the Internet. Article 11 applies not only to Internet users, but also to the operators of search engines, or any platforms which provide services intended to allow the discovery and exchange of information.

For the reasons mentioned above, it would be impossible for a data controller to comply with this obligation and we suggest the deletion of paragraph 2. Removing information from online publication is best achieved via data subject's requests to the publisher of that information, since the publisher is the person responsible for making the information public in the first place and can make it unavailable in the most efficient manner.

Data Portability

While we appreciate the provision's underlying intention of enabling users to switch their data from one service to another as easily as possible, we are concerned that this provision, if not well developed, may have a detrimental effect on both data subjects and data controllers.

Firstly, we take the view that data protection legislation is the wrong place to address such an issue. Secondly, 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, ignoring cases where organisations have the legal obligation to keep the data. Finally, due to the broad personal data definition, such a right risks leading to situations where companies could be forced to hand over information to competitors carrying significant commercial value or which have been created serving the purposes of the data controller only.

Some personal data have been generated on the basis of algorithms that are proprietary assets of the company. Granting a right to data portability for any type of data will lead to companies losing important competitive leverage and it risks killing any incentive to offer new innovative services to their users, which in turn will lead to less research and innovation, hence less functionality and service quality, thereby frustrating the user experience. It should also be noted that some deemed personal data include personal data of third party users.

As a result, we would highly recommend EU decision makers to delete the provision as it currently stands and carefully assess the issues of interoperability and transferability at stake. At the very least, it is of utmost importance to:

- Clarify that the scope of Article 18 does not impact the retention of personal data for compliance reasons or other legitimate purposes of the controller. In that respect, Article 18

should include a paragraph limiting the applicability of the right to data portability similar to the list of exceptions mentioned for the right to be forgotten;

- Make a distinction between user-generated data (i.e. information published by data subjects themselves such as name, email address, pictures, etc.), in relation to which portability is acceptable, and data that are the result of their interaction with the service providers, for which data portability should not be required.
- Leave it up to data controllers to decide on formats and technical details for data to be transmitted.

Accountability

Accountability is a well-established principle of data protection, found in existing guidance such as the Organisation for Economic Cooperation and Development (OECD) Guidelines[2] and Asia Pacific Economic Cooperation (APEC) Privacy Framework[3] and in the laws of for example Canada and Mexico. Regulators, industry and advocacy groups have further defined the essential elements of accountability[4]. According to the accountability principle, all organizations engaged in the processing of personal data, including controllers and processors irrespective of their size, should be held accountable for implementing appropriate, demonstrable and effective technical and organizational measures by means of a privacy program to ensure proper protection of personal data.

Essential elements of effective privacy programs include:

- Sufficient management oversight;
- Policies, processes and practices to make the policies effective;
- Risk assessment and mitigation planning procedures;
- Adequately skilled data protection staff;
- Awareness and training of staff;
- Internal enforcement;
- Issue response; and
- Remedies to those whose privacy has been put at risk.

Privacy programs should be tailored having regard to the type of the organization, the nature of the processed data and the state of the art of technologies and available methodologies, for example to carry out a data protection impact assessment.

EDiMA is not convinced by the manner in which the accountability principle has been incorporated into the Regulation. Indeed, the Commission has opted for an antiquated prescriptive and straightjacket set of *ex ante* compliance requirements, which lacks flexibility. Instead of effectively encouraging the use of privacy enhancing measures, it introduces new and onerous requirements that will substantially increase disproportionate administrative burden for businesses without any regard to the potential privacy risks.

Implementing the superior Accountability concept as described above in the Data Protection Regulation instead of the approach as currently proposed would in practice lead to improved data protection. It would help reduce the burden on businesses and DPAs. In addition, granting benefits to

[2] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
[3] http://www.apec.org/Groups/Committee-on-Trade-and Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
[4] http://www.informationpolicycentre.com/accountability-based_privacy_governance/

companies demonstrating a responsible approach to privacy will incentivize the use of privacy enhancing measures ('privacy by design').

Accordingly, a flexible, yet clear requirement of an effective data protection program should be established in the Regulation. Other administrative requirements as proposed in the Regulation should in return be reduced, in particular:

- **Documentation requirements**: This obligation is overly detailed, prescriptive and disproportionate. Documenting will be a very extensive process, especially when joint responsibility is introduced. The obligation will trigger high costs, also for low-risk processes.
- **Data Protection Impact Assessment (DPIA):** According to the Accountability concept, all processing of personal data should be planned appropriately, including the execution of risk assessments prior to commencing the processing. No specific type of DPIA should be mandated nor should the assessment obligation be reserved to any specific type of processing.
- **Prior consultation**: Prior consultation with DPAs should only take place when the processing is based on the legal grounds of either 'exercise of public authority' (Article 6(1)e) or the 'legitimate interests test' (Article 6(1)f) *and* the processing in question is likely to present specific significant risks to data subjects. This means for instance that a prior consultation should not be required when the processing is based on 'consent' (Article 6(1)a) or 'contract' (Article 6(1)b). The activity of DPAs can consequently be much more focused on ex-post controls rather than ex-ante clearance of processing operations.[5]
- **Data Protection Officer (DPO)**: For this requirement to be valuable in terms of Accountability without unnecessarily increasing the cost of compliance and administrative burdens on companies, the appointment of a DPO should 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.

Controller/Processor responsibilities in the context of cloud computing

The development and uptake of new technologies such as cloud computing in Europe will very much depend on whether the new EU Data Protection Framework is sufficiently clear, workable in practice and designed to accommodate the realities of new technologies such as cloud computing. Actors operating in the cloud need to know the extent of their EU data protection obligations, and the burdens placed on them need to be appropriate to their respective role(s).

We take the view that the proposed Data Protection Regulation, particularly the rules relating to the controller/processor concepts 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 those rules will impede rather than promote the further development of cloud computing services in Europe.

The traditional, rather static division of entities involved in the processing of personal data (controller-processor concept), which has been retained in the draft Regulation, does not sit well with today's sophisticated cloud environment with many different business models, multiple actors and layered arrangements between providers, and is therefore difficult to apply in practice. In fact, **in the cloud computing context, the traditional binary distinction between processors and controllers**

[5] Recommendations of the Article 29 Data Protection Working Party in its Opinion 3/2010, paragraphs 54 and 63.

is blurred and in some cases neither of these roles as they are defined today may necessarily be appropriate for some cloud providers.

While in the traditional information technology model an organization is accountable for all aspects of data protection – from how it uses personal information to how it stores and protects data kept on its own computers – cloud computing differs because information can flow offsite to data centers owned and managed by third parties, the cloud providers. For instance, some cloud providers that provide end-to-end data processing may in fact significantly influence the technical and organizational measures to be used for that data processing. On the other hand, where the cloud provider is offering simple infrastructure services to customers for their own data processing, the provider's involvement is very different to that of a traditional processor. These examples are reflective of the risk of inappropriate qualification of cloud actors, which can have far-reaching consequences for them in terms of responsibility and liability. Thus clearly defining the roles and allocating the distinct responsibilities and obligations for security and privacy among such actors is vital, and we would suggest recognition in the Regulation that there will be varying degree of responsibilities and liabilities among them.

Furthermore, there is a great deal of uncertainty in the Regulation with regards to the balance in responsibilities between controllers and processors. The concept as proposed imposes onerous new obligations on processors, extends some of controller responsibilities to the processor and imposes direct liability on the processor, thereby unduly eliminating the accepted distinction between controller and processor and disregarding the fact that only the controller has full picture of processing while the processor only sees isolated elements. The proposed paradigm shift could be prejudicial to cloud development and uptake in Europe. In addition, due to the specificities of some cloud business models, some providers will technically and practically not be able to comply with many of these new obligations.

To ensure that the Regulations takes account of the particularities of the cloud computing context and today's business reality and what is more, that it encourages the cloud development in Europe, we propose the following changes:

- **The data controller should be redefined as the one who determines the "purposes" of processing.** Given that in the context of new technologies processors are playing a greater role in determining the *means and conditions* of processing, we would urge that the definition of controller is limited to the one who determines the *purposes* of processing.
- **Clarify the balance between and extent of processor/controller obligations.** A robust data protection regime needs to clearly delineate the responsibilities of the different parties involved in processing information and ensure that the parties bear burdens that are appropriate to their role in the business ecosystem.
    - **The Regulation shall return to the current principle that primary and direct responsibility & liability for processing remains with the controller.** We therefore suggest deletion of any reference to processor in provisions concerning the controller's obligations (Article 22 et seqq.).
    - **The processor obligations and liabilities should be limited to the status quo**, namely the duty to provide for sufficient technical security measures and organizational safeguards regarding data processing. There should be no direct obligation and liability for processors beyond this and beyond what has been contractually agreed between the parties.
    - **Any regulatory allocation of responsibilities between controllers and processors needs to take account of the contractual arrangements** between them, in order to avoid potential

contradictions and overlapping responsibilities. It is important that the contractual freedom and flexibility for controller/processor agreements is preserved.

- **The new responsibilities for processors which do not provide clear benefits in terms of enhanced data protection should be removed.** Requirements such as obtaining prior authorization from the controller to enlist sub-processors are not workable in today's cloud context and impose burdens without adding clear benefits in terms of better data protection. We propose removing this requirement or further clarifying it in order to permit general consent by contract to use sub-processors. It should be clarified in Article 26(2) of the Regulation that it is up to the parties to contractually define the scope of the obligations mentioned therein. At a minimum, it should be clarified that these obligations only apply where the processor is able to assist the controller with reasonable effort and where this is possible given nature of processing and information available to him.
- **The allocation of obligations for processors and controllers should** not be left to secondary legislation in the form of delegated acts for actors to understand the responsibilities, duties and tasks that apply. For this reason, we propose to delete Article 26(5).
- **The Regulation should offer clear regulatory incentives to controllers and processors investing in security & privacy enhancing measures and making use of viable self-regulatory systems and certification schemes via waivers from administrative burdens and simplification mechanisms.** Cloud processors and others should be encouraged to go beyond the obligations in the EU law in certain contexts. Where controllers and processors propose additional safeguards to protect data, they should be incentivized to adopt these safeguards.

For example, we propose industry driven data protection seals and marks, that should be ***voluntary***, ***affordable***, ***capable of being rolled-out and recognized globally*** and ***neutral as to system, service or technology***. Also, the Regulation should stipulate that controllers using processors who offer additional legally binding safeguards, which are in line with (or go beyond) the industry standards, and who can demonstrate this via conclusive certificates (e.g. self-assessment via DPO, code of conduct, voluntary third party certification), could enjoy less prescriptive requirements (for example exemption from obligation to control compliance as referred to in Article 22(1) and 26(1)) or benefit from simplified mechanisms to transfer data. Other valuable tools to achieve such 'safe harbor' could be industry-developed standard contractual clauses offering sufficient safeguards in terms of EU privacy law to be approved with pan-EU effect by lead regulator. Such a system would allow for flexibility, legal certainty, less administrative burden for cloud provider, security and legal certainty for cloud customer, highest privacy and security standards for data subjects and transparency for regulators. It would set incentive to invest more in privacy enhancing measures, which in turn would increase the level of data protection.

Delegated acts

Through the new Regulation, the Commission is given substantial authority to adopt delegated acts and implementing acts in virtually every area covered by the proposal. These acts could include design requirements, technical standards, criteria for technical measures, and requirements for many of the most important obligations imposed on businesses. Among these acts, some may also be sector specific.

We acknowledge the Commission's efforts to bring a balanced policy approach to policy making in the area of data protection through delegated acts. This will help reduce the risk of policy being made by default by the Article 29 Working Party by ensuring that the Commission brings its horizontal policy mandate to bear. However, we are concerned about the fact that the scale of the

Commission's ability to propose secondary legislation in a wide number of areas threatens to complicate, rather than simplify, data protection. Adopting highly prescriptive measures or imposing specific technology outcomes via delegated acts could potentially impede innovation in privacy protection. Accordingly, we believe that:

- Given their wide reach, greater certainty as to how these acts will work is essential. In particular, care must be taken to ensure that the process is transparent and inclusive, notably with regard to industry participation.
- At a minimum, the Regulation should make clear that any secondary rules do not take the form of design mandates or preferences for particular technology solutions.
- The proposal fails to set out a timetable for the adoption of such acts, undermining predictability and creating business uncertainty. We thus recommend that a specified deadline for each delegated act provision should be put in place by the Regulation, according to which the Commission should submit legislative proposals.
- The sheer weight of delegated acts as proposed is not manageable. We recommend that attention be given to reducing the number of areas for which a delegated acts procedure is foreseen. This could be done in a variety of ways, including simple deletions, replacements with other procedures, or in some cases direct insertion of relevant provisions in the legislative text. At a minimum, we recommend that delegated acts that deal with essential elements of the law, as well as those that threaten technology neutrality should be deleted.

For more information, please contact the EDiMA Secretariat: info@europeandigitalmedia.org
Tel: +32 (0)2 626 19 90 Fax: +32(0)2 626 9501