



# **CONSULTATION ON THE COMMISSION'S COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION**

**JANUARY 2011**

## **1 INTRODUCTION**

EuroISPA welcomes the opportunity to contribute to the discussions surrounding the review of the legislative framework for data protection. Our contribution tries to address what we consider to be the most important issues raised in the Communication on “A comprehensive approach on personal data protection in the European Union”.

EuroISPA believes in the need to preserve the principles-based approach of the Directive. It provides for the needed flexibility to face future technological developments as long as a coordinated approach is adopted at EU level.

EuroISPA considers that it is important to address the impact that future innovations can produce on privacy through non-legislative measures, such as the use of privacy-enhancing technologies, privacy-by-design and industry self-regulation which are the most effective means to deal with fast moving technology markets. Legislative measures that are not technology-neutral could act as a barrier to innovation and deprive consumers of valuable products and services.

We also believe that data protection rules should be applying horizontally to all economic sectors and actors processing personal data which impact on the privacy of individuals. A level playing field is essential to build uniform expectations and experiences online while increasing the confidence on using online services.

Finally, EuroISPA welcomes the reference in the Commission's Communication to privacy information notices and the extension of data protection rules to the area of police and judicial cooperation on criminal matters, and its members remain willing partners in actively contributing to future discussions.

## **2 LACK OF HARMONISATION**

The Directive has failed in creating a harmonised framework across the EU, as also acknowledged by the Commission in its Communication. Member States have implemented it in divergent ways with the consequence of creating obstacles to the establishment of the Single Market. The efforts of the Article 29 Working Party in the achievement of a consistent interpretation of the provisions of the Directive have not succeeded, so far, in preventing its fragmented application<sup>1</sup>. Bureaucratic obstacles to the free movement of data are also inhibiting the development of cloud computing. The latest issue of INSEAD/WEF Global Information Technology Report estimates that comprehensive diffusion of cloud computing could cut the

---

<sup>1</sup> As an example, the implementation of the “explicit consent of the client” is different between G29 and the French national authority.

fixed costs of European firms by 5%, raise GDP by up to 0.3% and create about a million additional jobs<sup>2</sup>.

In a truly harmonised data privacy framework, EU-based data controllers would not be prevented from moving data freely within EU borders. Any restrictions are contrary to the obligations imposed on Member States by Article 1 (2) of the Directive 95/46/EC.

### **3 APPLICABLE LAW**

The definition of the applicable law is a key question in a globalised online environment, where the most frequent scenario allows the collection and processing of data belonging to European citizens by extra-EU entities. Article 4 of the Directive 95/46/EC already addressed this issue stating that the Directive is applicable to data processing anywhere and, therefore, also outside the EU (a) when the controller is established in the EU, or (b) when the controller is established outside the EU but uses equipment in the EU.

EuroISPA believes in the need of a legal framework that can be applied across borders, which gives users the means to exercise their rights across borders, which is based on the concept of accountability and draws on technological controls and self regulatory codes, and mechanisms as supported by Articles 17 and 27 of the Directive 95/46/EC.

Higher legal of certainty and better harmonization in the application of EU data protection laws is very important. EuroISPA suggests that applicable rules for the companies operating across multiple EU Member States be the one of its main establishment, from where its operations are lead.

We believe that accountability should be based less on prescriptive legislation and regulation and more on the adoption, commitment to and practice of core internationally recognized privacy principles and information governance standards. To this regard, EuroISPA considers that Recital 2 of the Directive 95/46/EC stating that “data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals” still remains valid today.

### **4 TRANSPARENCY IN PROCESSING**

The word ‘transparency’ is mentioned only once in the Directive 95/46/EC and is not mentioned at all in other applicable Directives, i.e. 2002/58/EC or 2006/24/EC. The industry supports an explicit requirement on responsible persons for ensuring the privacy of users and the protection of their personal information. Users now sit in a complex web of relationships with service providers often scattered around the world and sometimes operating from jurisdictions with incompatible or non-existent data privacy legal frameworks. EuroISPA believes that any new or amended legal framework must address the responsibilities of all actors across the global information ecosystem and the international dimension of products, services and information flows. However, EuroISPA does not believe that it is desirable or necessary for detailed rules to be drawn up regarding how transparency is to be provided. This would be extremely difficult to do in a reality where there is a limitless number of radically different contexts for data collection and use, and would be likely to result in many practices that add no value for the consumer.

---

<sup>2</sup> Soumitra Dutta (INSEAD) and Irene Mia, “Global Information Technology Report 2009-2010”, World Economic Forum: <http://www.networkedreadiness.com/gitr/main/fullreport/index.html>.

## **5 PERSONAL DATA OF MINORS**

In the online world young people are becoming increasingly aware of the privacy implications and consequences of engagement, and are actively managing their privacy. EuroISPA believes that emphasis should be put on awareness and education efforts and self-regulatory approaches to specific services or contexts that may impact on the privacy of minors, combined with guidance that promotes a harmonised approach.

## **6 PERSONAL DATA BREACH NOTIFICATION**

The revision of the Directive should be the occasion to amend and simplify the data breaches notification process and extend security breach notification requirements to all sectors, including for example, law enforcement agencies, online banking, schools and health services. EuroISPA also believes that security breach notification requirements should also be harmonised. However, it is important that detailed engagement begins with key stakeholders through an expert group to ensure a pragmatic, harm-based approach. A particular focus should be put on answering the following questions:

- What data types should the obligation apply to?
- What type of harm and thresholds of harm should apply?
- Should the obligations apply to data that has been encrypted or only to unencrypted data?
- What is the role of national data protection authorities and their jurisdiction over such matters?
- What are the timings of notifications to DPAs and/or individuals?
- Who should notify data subjects – the data controller or a DPA?
- Should the requirements apply to the ‘unlawful destruction’ or ‘alteration’ of data?

An in depth reflection and discussion on the questions with an expert group is essential to ensure that the benefits of data breach notifications are not counterproductive and do not unnecessarily affect end users’ trust and confidence. Notices should be carefully defined to avoid that notice obligations are applied too broadly, including to instances that do not represent a risk of harm, to avoid overloading consumers with (irrelevant) large volumes of notices and ultimately defeating their initial purpose.

## **7 RIGHT TO BE FORGOTTEN**

The right for the individual to request deletion of his/her personal data already exists under Article 12 of Directive 95/46/EC which provides individuals with a qualified right to request their personal data be rectified, blocked or erased. Some Member States have implemented the Directive in ways that obliges data controllers to meet such a request unless there is a justified reason for not doing so. This regime is supported by redress mechanisms which give the individual the right to ask the data protection authority to assess the refusal of requests to erase data which also gives the individual the right to pursue any such refusals via the courts. EuroISPA considers this framework satisfactory and does not see any need to amend it.

E-communications service providers are also subject to strict rules under the e-Privacy Directive 2002/58/EC which requires such providers to delete or anonymise communications data when those data are no longer needed for legitimate business purposes.

Furthermore, the right to be forgotten is also strengthened by the concept of “data minimisation” (only collecting and retaining personal data for legitimate purposes), which already exists in the Directive 95/46/EC.

## **8 DATA PORTABILITY**

A right to the portability of personal data exists in that individuals have the right of access their personal data pursuant to Article 12 of Directive 95/46/EC and implementation laws, and to be given a copy of that data. EuroISPA does not see any need for further regulation in this field, but recognises that further investigation is required to examine whether and how such a consumer prerogative could be exercised.

## **9 EDUCATION AND AWARENESS RAISING**

EuroISPA stresses the importance of informing data subjects about the privacy impact of their behaviours in the online environment. Indeed, in order to make data protection rules fully effective, education and awareness-raising initiatives should be promoted by both public and private sectors. Member States are already obliged by Article 14 of the Directive 95/46/EC to ensure data subjects are aware of their rights. EuroISPA believes it is for national DPAs via the Article 29 Working Party to establish positive working relations with key stakeholders to understand the degree to which further awareness raising is needed and how it may be improved.

## **10 CONSENT**

Effective, future-proof data protection rules should not impede, but rather support the development of new services for the benefit of consumers and governments, while, at the same time, supporting a uniform privacy protective and enabling framework for users. Over-regulation and over-protection is not the way to achieve effective data protection law.

EuroISPA notes that under the existing legal framework, data subject consent is only one of the possible bases for legitimate processing of personal data. This is an important legal principle that we believe should remain in place.

EuroISPA is concerned that requiring explicit prior consent for all processing will ultimately undermine privacy. Privacy is dynamic and contextual – it is not static. Rather than focusing on consent at the expense of other opportunities to enhance a user's privacy experience, EuroISPA believes that a key objective for data controllers should be to develop the mechanisms by which users can make informed choices depending on the context of specific uses of data. For example, a person requesting a location based information service to locate the nearest automatic teller machine, is actively asking to be located, and should not be required to negotiate cumbersome, lengthy legalistic privacy notices by which they may indicate their 'unambiguous explicit consent'. Such impositions would damage the user experience and do little, if anything, to enhance the user privacy experience. However, should the location based service provider wish to retain information about the use of the service in a non-anonymised form for the purposes of targeting the user at a later stage with offers, then the service provider would be expected to provide the user with a short contextual notice to this effect and ensure the user is able to express his choice and preference.

EuroISPA agrees with the need to avoid ambiguous and confusing information or even an absence of information but does not consider that consent must always be prior. With regard to the e-communications sector, and after long discussions during the adoption process of the Directive 139/2009/EC on e-Privacy, the legislator agreed that the final text should not include the word "prior". In addition, the recently published Communications Committee (COCOM) Guidance on implementation of the e-privacy directive to Member States confirms this fact<sup>3</sup>. The adoption of a rigid approach would risk hindering the establishment of a harmonised privacy framework. Indeed the importance of the temporal aspect of consent should not outweigh the

<sup>3</sup> Communications Committee's Implementation of the revised Framework Article 5(3) of the ePrivacy Directive : [http://circa.europa.eu/Public/irc/infso/cocom1/library?l=public\\_documents\\_2010/cocom10-34\\_guidance/ EN\\_1.0\\_&a=d](http://circa.europa.eu/Public/irc/infso/cocom1/library?l=public_documents_2010/cocom10-34_guidance/ EN_1.0_&a=d)

importance of the “informed” nature of consent. The legislative framework should acknowledge that consent does not necessarily have to be provided prior to the collection and use of personal data, but that it should be properly informed.

## **11 PROFILING**

Profiling supports a wide range of legitimate activities across a number of key sectors, including banking, telecommunications, the Internet and all other sectors in which the ability to understand customers’ use of services is central to ensuring they can respond to consumers’ needs and demands.

The e-communications industry believes that Article 15 of Directive 95/46/EC does not support prohibiting ‘profiling’. Any decisions to change this article require a thorough understanding of the term, its applications and the impact on society and individuals. A dialogue to improve the Commission’s knowledge of business practices and the benefits of profiling would be extremely beneficial.

A prohibition on profiling may also interfere with certain aspects of an individual’s right of informational self-determination. For example, would a prohibition on profiling prevent an organisation from offering and a user from asking to receive benefits from the analysis and profiling of the user’s data?

On the basis of all of the above, EuroISPA calls for a clear support for universally recognized privacy principles such as transparency and user control in the data protection revised framework.

## **12 INTERNATIONAL TRANSFER OF DATA**

The current rigid EU rules applying to the transfer of data to third countries do not seem adequate for the cross-border data flows in a globalised economy. In complex situations, with multiple data controllers involved (e.g. cloud computing) the current provisions of the Directive may severely impede the international transfer of personal data and, thus, the activities of EU companies worldwide. The framework should provide simple tools for compliance and move away from bureaucratic approaches to enforcement. Likewise, the framework should restrict the ability of Member States to subject international data transfers to additional local requirements, if the organization is transferring the data outside the EU in compliance with established EU rules.

Since the adoption of the Directive, experience shows that Binding Corporate Rules solutions for inter-group transfers are also cumbersome and should be updated to make it simpler for groups of companies to adopt. The EU legal framework should recognise the concept of “group of companies” in order to facilitate the transfer of data between members of the same group, irrespective of whether they act as processors or controllers. This would be an important step in reducing the administrative burden of EU businesses. Therefore, EuroISPA very much welcomes the reference, for the first time, to “transfer carried out within corporations or multinational groups” in the Madrid Resolution and asks the Commission to follow this positive approach. Internal Privacy Policies of such multinational groups would then include the guarantees that the transferred personal data will benefit from the same level of protection as if they were processed within the EU borders.

Despite the dynamics of the sector and the increasing changes to the role of data controllers and processors, Binding Corporate Rules currently only apply to data controllers. A review of the Directive should therefore recognize these needs and include similar approach tools for the processing of personal data by pan-European and multi-national players (e.g. Binding Safe Processor Rules).

## **13 ADEQUACY PRINCIPLE**

As the adequacy principle is concerned, it has proved to be ineffective and too limited, as shown by the small number of countries deemed to have adequate legal frameworks, amounting *de facto* more to an equivalence test. Additionally, the administrative practices required for getting Standard Contractual Clauses, model contracts or Binding Corporate Rules, need to be improved. In this regard, a reasonable time scale for assessment and approval, a reduction of costs, together with increased transparency from both the requesting company and the relevant authorities involved would contribute to harmonisation while guaranteeing an adequate level of protection.

## **14 SELF-REGULATION**

EuroISPA is of the view that self-regulation premised on a privacy-by-design approach, which includes the principle of accountability and recognises the dynamic contextual nature of privacy, can work to ensure individuals are both aware of and able to exercise their various rights. In our view, self-regulation is able to respond in a more timely and effective manner to changes in technology and business models than ex-ante legislation. However, in order to develop self-regulation, further harmonisation and clarity of rules among Member States are crucial. Indeed, even where self-regulation is encouraged by the Directive, some Member States do not leave room within the national legal framework for it to flourish and this is one of the main reasons that prevented the elaboration of codes of conduct.

EuroISPA notes that EU data protection law does not give Member States legal certainty that allowing self-regulation by industry allows them to fulfill their legal obligations to implement EU law under the Treaties. A clarification that self-regulation can allow for the fulfillment of Member State obligations would be helpful. Moreover, Article 27 of the Data Protection Directive provides for dialogue between industry and DPAs with regards to codes of conduct. However, it does not clearly define roles and responsibilities, and it does not address important questions about the relationship between national and EU law.

EuroISPA believes that if the Commission is intentioned to actively promote self-regulation or EU certification schemes, this should be done in close cooperation with the industry through an expert group to ensure a pragmatic approach.

## **15 ROLE OF DATA CONTROLLER AND DATA PROCESSOR**

The distinction between data controller and data processor is changing in the online environment and becoming outdated with the development of cloud computing, outsourcings and sub-processings. It is even more frequent that several parties are defined as “controller jointly with others” as they determine “the purposes and means of the processing” (Article 2 of the Directive). In order to address these changes, EuroISPA believes that the data controller’s obligations should be made more flexible and that contractual clauses with regard to the obligations between data controller and data processor should be permitted.

## **16 REDUCTION OF ADMINISTRATIVE BURDENS**

The obligation on data controllers to notify Data Protection Authorities (DPAs) of the processing of personal data amounts to an increase in the administrative notification duties without any real advantage for DPAs and data subjects. EuroISPA believes that in order to address this concern, possible solutions could be considered such as:

(i) a mutual recognition of a notification by a DPA in a country could make further steps in other Member States unnecessary: this would allow a reduction in resource-consuming notification processes; or

(ii) the reduction of the burden of the notification obligation by adopting the possibilities provided in Article 18 (2) of the Directive (Exemption from notification).

As a general rule, the notification should be required only in cases of notable risk or harm, or when transparency cannot be adequately ensured via other means.

These solutions would allow the data controller to focus more on the “effective” protection of data, while relieving DPAs from unnecessary formal requirements.

## **17 INTERMEDIARY LIABILITY UNDER THE DATA PROTECTION DIRECTIVE**

When the data protection Directive was drafted, almost sixteen years ago, the Internet was in its infancy. Web 2.0 services were completely unknown at legislative level to be even taken into account in the Directive. Today these services are those that generate the most of the online traffic and are an unprecedented means to allow access to information and promote the exercise of fundamental rights. Internet Service Providers have played an essential role in allowing the creation of these services and ensuring the exercise of those rights. In this context, the intermediary liability protection granted by the Electronic Commerce Directive 2000/31/EC (ECD) determined the conditions by which intermediaries’ liability of providers will be limited. However, an interaction between the Data Protection and ECD Directives, difficult to foresee eleven years ago, is now needed in order to ensure a proper protection of privacy of communications while fostering innovation within the Internet environment.

Indeed, in many instances intermediaries are processors of data and, therefore, acting entirely on behalf of the data controller. In these cases, it should be clear that the ultimate responsibility to assure compliance with the data protection law relies on the data controller. In general, we believe that while service providers should be held responsible for their own collection and use of personal data of individuals, to preserve the intermediaries’ vital role in the information society the intermediary responsibility needs to be limited where it concerns data protection issues related to third party use of online services. Intermediaries’ responsibility or direct liability for privacy violations committed by third parties would have a deleterious effect on the free flow of information and innovation of online services.

As intermediaries enable access to information, sharing and hosting third party content, the question of liability for harm to individuals on the basis of privacy and data protection violations becomes imperative.

Unfortunately, the ECD explicitly excluded from its scope cases where privacy and data protection are involved:

Article 1 (5): *“This Directive shall not apply to:*

*(b) questions relating to information society services covered by Directive 95/46/EC [...]*”

Nor was the concept of intermediaries considered when the Data Protection Directive was drafted. The lack of clarity in the interpretation of the EU acquis could lead to serious consequences of intermediaries such as the demonstrated risk that Member States could hold intermediaries fully liable for data protection violations by third parties.

To give an example, if a user uploads a video on an online platform, the provider will host the data (and/or personal data) on its server on behalf of the user. However, it is not clear if such platform is either a controller or rather a processor of the data “posted” by its user online. This creates legal uncertainty for online intermediaries. Indeed, if the uploaded video is harmful to

the privacy of a third party, under the existing legal framework (E-Commerce Directive), the provider would not be liable if it removed swiftly the content after having actual knowledge of its illegality (so called notice and take-down). However, since the ECD liability limitations do not seem to be applicable to data protection, and in absence of an explicit clarification in EU law, the same provider would risk being liable for breach of personal data rules by third parties. To prevent this occurrence from happening, the only possibility a provider has to avoid liability would be to constantly monitor all the content uploaded by its users with subsequently leading to massive censorship.

The unintended consequences stemming from making an Internet provider liable for privacy rules violations of its users should be prevented. The system set in the ECD is sufficiently flexible to protect Internet providers and ensure accountability of users for their actions, while preserving the incentives online business have to innovation.

EuroISPA believes that failing to recognize the role of intermediaries could lead to an obligation to general monitoring of the Internet. This outcome was clearly ruled out in the ECD, because it would seriously hamper the viability of the Internet and because it could have implications on privacy that outweigh the aims of such monitoring. Therefore, we believe the review of the Directive 95/46/EC is a good opportunity to address this issue and recognize through legislative changes or otherwise that intermediaries as defined in the E-Commerce Directive should have at least the same liability limitations regime for the purposes of privacy and data protection violations of third party content as the ones outlined in the E-Commerce Directive itself.

## **18 THE ROLE OF LAW ENFORCEMENT**

EuroISPA would like to stress again that today e-communications providers are faced with high administrative burdens, with associated compliance costs due to differences between processes in each of the Member States. On the other hand, the benefit of strong data protection rules to consumers is not being maximised, because enforcement resources are not focused on the avoidance of consumer harm. We believe that if DPAs were able to adopt a more outcome-focused approach whilst lowering administrative burdens, consumers would be better protected by the framework.

Therefore, EuroISPA calls for the introduction of an ex-post, market surveillance and harm-focused approach to give enforcers and companies engaged in data transfer more flexibility and maximise the effects of enforcement and consumer benefits.

Additionally, Internet Service Providers should not be put in situations of unfair liability for data provided to national law enforcement authorities. Such authorities should take clear responsibility for the economic costs to Internet Service Providers of data retention and provision, and should also be clearly responsible for any consequences for civil liberties or Human Rights violations.

## **19 THE ROLE OF THE ARTICLE 29 WORKING PARTY**

EuroISPA believes that this review provides the opportunity to define a better interpretation of the legal framework that takes into account the Internal Market dimension and puts privacy legislation in the context of other EU policy objectives and instruments.

EuroISPA acknowledges the Article 29 Working Party efforts to achieve an increased harmonisation and coordination in the application of the Directive. However, we believe that, in order to achieve such a goal, the Commission needs to be given more interpretative powers, while still taking advantage of the advisory role of the Article 29 Working Party. We also consider that further involvement of the private sector in the activity of the Article 29 Working Party is necessary. The Article 29 Working Party should be more transparent and accountable

for the decisions and opinions adopted, and should seek to ensure views of key stakeholders are considered wherever possible.

The Article 29 Working Party should also be required to assess the degree to which the data privacy Directives have been interpreted and applied in ways that achieve harmonisation across Member States. An example of a lack of harmonisation is the position of German DPAs who have determined that the use of Google Analytics is illegal while the UK DPA advises visitors to its website that it uses Google analytics to “help analyse use of [its] website”. Such inconsistencies are confusing for individuals and businesses, and not conducive to encouraging confidence in those responsible for developing privacy policies. The Article 29 Working Party should be required to publish the findings of such assessments to aid the Commission in its decision-making.

## **20 CONCLUSION**

EuroISPA strongly believes that the Directive 95/46/EC has played a crucial role in protecting the rights of individuals and offering mechanisms for businesses to maintain consumer confidence. Nevertheless, the divergences in implementation across Member States have raised barriers for the completion of the Single Market. Additionally, a flexible framework that allows businesses to create and offer products and services at an international level, while ensuring that data subjects maintain their right to an efficient data protection through effective enforcement and accountability mechanisms, has yet to be achieved.

EuroISPA considers that it is important that a revised legal framework benefits users and businesses and is globally relevant and effective. It is also critical that the European Union avoids the temptation to address the challenges of the global Internet by walling itself off from the rest of the world. Such a posture would undermine innovation and global offering of products and services online.

### **EUROISPA**

EuroISPA is the world's largest association of Internet Service Providers (ISPs), representing the interests of over 1800 ISPs across Europe. With a Secretariat in Brussels, EuroISPA is a major voice of the Internet industry on information society subjects such as cybercrime, data protection, e-commerce regulation, EU telecommunications law and safe use of the Internet. Further information about the organisation (including its composition, aims and position papers) is available on its website: <http://www.euroispa.org>.