



## **FEEDBACK TO THE COM(2010) 609 FINAL: A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION**

The European Privacy Association (EPA) brings together experts on Privacy and Data Protection from across Europe and represents a unique European platform enhancing dialogue among all stakeholders, such as decision-makers, researchers, privacy commissions, NGOs, industry and the media.

EPA informs and educates the general public about industry efforts to improve privacy, e-security and data protection, providing a unified response to public concerns. Extremely aware of the global aspect of privacy and data protection, EPA develops policies and produces legal and scientific positions engaging with policymakers at every level across Europe: the European Parliament, the Commission, Member State regulatory authorities and international organizations.

EPA activity is primarily focused on cybersecurity, online ads and profiling, cloud computing, mobility, e-government and citizens data, RFID, privacy, terrorism, spamming, search engines, social networks, and the economy of human information.

## Introduction

EPA is thrilled to contribute to the Commission's consultation on a *Comprehensive approach on personal data protection in the European Union*. The issue is important not only as stronger and more effective protection is essential to match changing technology, but also as further harmonisation of data protection rules can ensure a level playing field for companies, data subjects and data controllers.

The response that follows aims to enhance the debate and represents a contribution to the work that the Commission and the various European stakeholders have undertaken during the last years. EPA's contribution seeks to address some of the critical challenges we will face in the near future, in particular those related to cloud computing and cyber security which have crucial privacy implications. It is essential to initiate a serious reflection on the role of technologies in our society, as privacy is an individual right, but also an essential instrument to improve our lives and prosperity. We believe the current revision of the Directive 95/46/EC represents a great opportunity to concretely address such challenges, providing sustainable solutions aimed at guaranteeing the right to privacy and data protection.

EPA pursues a pan-European approach. The contribution that follows reflects the ideas and thoughts of several European fellows that deal everyday with privacy and data protection issues in their capacity as privacy experts, in academia, law and business.

**The Italian Institute for Privacy** (Istituto Italiano Privacy - **IIP**) and the **Spanish Privacy Professional Association** (Asociacion Profesional Espanola de Privacidad, **APEP**) also contributed to this submission. EPA aims to represent the voices of various European stakeholders engaged with privacy in different cultural, economic and social contexts around Europe.

EPA wishes to thank all individuals and organizations that have provided ideas and thoughts to this contribution and for the support they bring to the work of the Association every day.

## **European Privacy Association (EPA)**

### *2.1.2 Increasing transparency to the data subjects*

To make the information on data processing easier to understand, more transparent, and more accessible to the data subjects the Commission should also consider:

a) Developing a number of icons symbolizing what kind of processing is carried out by the controller and how (e.g., profiling, behavioural advertising, transferring of data outside the EEA) and how to exercise data subject rights (e.g., by email, by online form). A source of inspiration could be the Pan European Game Information (PEGI) content rating system, as far as the icons symbolizing the content of the game are concerned ([www.pegi.info](http://www.pegi.info)). Such icons could be showed on the controller website and relevant privacy documents;

b) (on the web) consider the possibility for the controller to provide privacy information by means of an audio-video clip, where the principal elements of the processing carried out by the operator will be provided in clear and plain language; and, for the full version of the information privacy notice to be displayed, referring to the relevant page/document.

### *2.1.3 Enhancing control over one's own data*

Data subject rights should not only be made more explicit, clarified and possibly strengthened, but also harmonize the way these rights can be exercised. This will not only be relevant for data subjects but also for multinational companies - acting as data controllers - established in several Member States that, at present, have to offer multiple ways for the data subjects to exercise their rights in different Member States – generating extra cost that should be avoided in the Internal Market.

### *2.1.4 Rising awareness*

The Commission may also want to consider whether to request that controllers communicate awareness-raising activities carried out by the relevant Data Protection Authorities (DPA). In this way, DPAs will be aware of such initiatives in their territories and possibly cooperate in carrying efforts to educate users/consumers.

### *2.1.5 Ensuring informed and free consent*

As far as the rules on consent are concerned, the Commission should not only clarify and strengthen privacy rules, but also ensure a common interpretation throughout the Member States. The current inconsistent interpretation of consent requirements throughout the Member States is not only detrimental for data subject awareness on whether s/he is consenting and to what processes they are consenting, but also generates extra costs for multinational companies - acting as data controllers - established in several Member States that should not exist in the Internal Market.

### *2.2.1 Increasing legal certainty and providing a level playing field for data controllers*

We strongly welcome the Commission effort to examine means of achieving further harmonisation of data protection rules at the European level. As stressed above, harmonization is key not only for data subjects but also for multinational companies established in several Member States that: (i) have to bear extra costs to cope with inconsistent rules on data protection; and (ii) have no certainty of satisfying data protection duties and obligations. This should, of course, be avoided in the Internal Market, not least because it represents a competitive disadvantage for companies - acting as controllers - established in the EU in contrast to their competitors established outside the EU.

### *2.2.3 Clarifying the rules on applicable law and Member States' responsibility*

At present, multinational companies - acting as data controllers - established in several Member States have to comply with the data protection law of each of the Member States where they are established. This has resulted in significant compliance costs for such companies - that should not exist in the Internal Market - without generating significant benefit for data subjects. The aim should be to guarantee that companies will be able to process data, subject to a single set of rules across the EU.

#### *2.2.4 Enhancing data controllers' responsibility*

We strongly welcome the definition of the 'Privacy by Design' principle. In fact, it will give controllers a sense of responsibility in the development of new products and services, which will help the evolution of a market that is compliant with data protection rules.

#### *2.2.5 Encouraging self-regulatory initiatives and exploring EU certification schemes*

We strongly welcome co-regulation initiatives in which controllers cooperate with the Commission or the local DPAs on viable codes of conduct and, more generally, to enhance compliance and improve enforcement of data protection rules.

We also welcome the Commission's commitment to exploring EU certification schemes (e.g., 'privacy seals') for 'privacy-compliant' processes, technology, products, and services – as an expression of the self-regulatory mechanism already stated in the Directive 95/46/EC. Trustmarks or seals (depending on how one calls them) are very valuable, easy-to-recognise tools to communicate data protection compliance to users/customers.

However, the Commission should ensure the development of trustworthy European privacy seals, as most of the privacy trustmarks (seals) are, at present, not the result of a trustworthy certification practice<sup>1</sup>. In this effort, the Commission should aim at voluntary EU certification schemes, which will be affordable, technology neutral, and globally recognised.

#### *2.4.1 Clarifying and simplifying the rules for international data transfers*

We strongly welcome the Commission's commitment to improving and streamlining the current procedure for international data transfers in order to ensure a more uniform and coherent EU approach vis-à-vis third countries and international organizations. Greater legal certainty in the application of EU data protection laws must be a priority to protect the interests of EU citizens.

The present limited and sometimes inadequate means for the lawful transfer of personal data to controllers or processors - established in countries outside the EEA - represents an obstacle for the competitiveness of EU-based online service providers. The cloud-computing environment is a clear example of a sector in which the current legal means for transferring personal data outside of the EEA falls short, and thus improvements in this respect are needed. Accordingly we think that the Commission should take into account one applicable law for organisations operating across multiple Member States by enabling them to comply with only a single EU Member State's law. A criterion in many for determining the relevant law to apply could be that of the main establishment. In the cloud-computing environment this would be the physical location of the data centre where data are stored and managed.

#### *2.4.2 Promoting universal principles*

We strongly welcome the Commission's commitment to enhancing its cooperation with third countries and international organizations, such as the OECD, the Council of Europe, the United Nations, and other regional organizations.

We believe that, nowadays, data protection issues should be addressed at the global level from the outset.

#### *Extra: Definition of controller and processor*

At present, there are some situations where it is very difficult to clearly define the data protection roles in processing. One of the most critical examples is represented by the data processing in the 'cloud-computing environment'. The Article 29 Data Protection Working Party: Opinion 1/2010 on the Concepts of "Controller" and "Processor" has not provided clear guidance in this sense. We strongly recommend further clarification on this matter by the Working Party. It is crucial to clearly be able to identify data protection roles in order to identify relevant duties and obligations and to allocate responsibilities – especially in a complex and fast growing market as represented by cloud-computing services.

---

<sup>1</sup> See extensively on trustmarks, Balboni, P. (2009) Trustmarks in E-Commerce: The Value of Web Seals and the Liability of their Providers, T.M.C. Asser Press, The Hague, 240 pages.

## APEP Contribution

### I. Modernization of the personal data regime

#### a. A dynamic definition of personal data: subjective and objective definition

The personal data definition requires a dynamic approach: it is not only important to determine which information identifies or may identify an individual but also who is the one that /who may carry out such identification in each context.

For example, if a controller codifies personal data (reversible dissociation) before transferring the codified data to a certain recipient (potentially, a controller or a processor), as long as the recipient cannot (legally) access (and/or is prevented contractually to have such an access) to the codes which enable to link the codified information to the personal data, it must be understood that no personal data transfer occurs. Therefore, the data protection regulations must apply to the dissociation procedure (in this case, the codification procedure) but not to the transfer itself.

This dynamic approach must also be considered when analysing IP addresses or localization data which do not identify *per se* an individual even though privacy (rather than data protection) concerns arise. Clear criteria must exist to determine when an IP address or localization data gathered through the Internet or RFID devices are personal data. To avoid this dynamic approach and to qualify almost everything as personal data do not provide proper responses to the harms caused by the use of such "non personal information" and may avoid the proper development of certain benefits of the digital society. The data protection regime cannot and should not provide the responses to all the threats of the digital society. Data protection and privacy are sometimes related rights but they are distinct rights that deserve a different treatment. Therefore, to impose restrictions on invisible and unauthorized tracking is necessary but it does not mean that such regulation should consist of applying all existing data protection principles.

#### b. Controllers not established in the EU and article 4.1.c) of the Directive: must the equipment location be replaced by other criteria?

For controllers not established in the EU, the existence of the processing equipment in the EU territory triggers the application of the Directive. If it is considered that this criteria still proves to be useful, there is an urgent need to harmonize what the "equipment" should mean and, in particular, whether the existence of a processor could qualify as such (the Spanish DPA has sustained it, for example).

However, the first question to be posed is to whether the data protection applicability criteria (mainly, the link between the data controller's establishment or with the EU) must be changed to the one used in other related regulations, such as the information society services, which refers to the market to which the information society provider addresses its services. The market criteria seems to be a better approach to follow, since the personal data is not only a fundamental right (as currently acknowledged by the Lisbon Treaty) but also a business asset. The opinion of the Article 29 Working Party to qualify the "cookies" as the equipment relevant for the EU data protection regimes to apply is a good example of an inadequate construction of the current criteria of the Directive in an attempt to provide a legal solution for this kind of (personal data?) "processing".

In addition, the modification of the Directive must make the technological neutrality principle true. For example, there is no reason to have different regimes for direct marketing depending on which channel used. The different applicability criteria on commercial communications used under the regulations on data protection, information society services, telecommunications, consumers and unfair competition have lead to a very complex and, thus, useless, regime (at least in Spain): tacit or explicit consent if sent by postal letter, explicit consent if sent by e-communication means (unless the soft

opt-in applies), explicit consent (with no exceptions) if sent by fax or automated calls, ...

**c. The household exception**

Social networks are main interaction channels of our 2.0 society. User do not (only) need to be protected from the public powers, not even from private multinationals ... but from others users!

To qualify a user of a social network that have more than 400 “friends” as a controller does not provide the solution. If the concept of controller could prove to be of assistance, each of the obligations attributed to a controlled must be nuanced in this context, and sometimes excluded. To acknowledge rights to users enforceable *vis-à-vis* other users, such as the right of rectification or cancellation/deletion or to attribute a compulsory role in this respect to the social network organizer (following, for example, some cease-and-desist models for copyright alleged infringements) do not mean that it has any sense to also have any user registering its “friends” database before a DPA or including a “data protection” notice in its wall.

**d. The group concept**

Only the BCR have examined to a certain extent the intra-group transfers and they have proved to be, in practice, a useless tool. And one of the reasons is due to its lack of specific recognition in a EU law to be implemented in the Member States or directly applicable to them and, thus, the difficulty of ensuring that the rules are binding externally according to the same criteria shared by all the EU DPAs.

It is therefore the right time to address the external binding nature of the BCRs in the EU regulations and whether the mutual recognition principle or a figure with similar effects may have a place in the data protection regime that must exist under the Lisbon treaty.

**II. The enhancement of rights requires to have a “European” personal data single market:**

**a. A single notification throughout the EU**

Global operators cannot but welcome the idea of a single notification throughout the EU. This entails that the harmonization must at least refer to the “unit” of notification: the controller, a controlled processing (exclusions?) or a controlled database?

In all events, the concept of personal data itself is also concerned. In addition to the above comments on the dynamic approach, an additional question that must be clarified regarding individual businessmen/women or the professional details of the individuals working for a certain legal entity (whether through a labour or professional services relationship) processed for a B2B relationship.

For example, the Spanish approach is far from being clear regarding individual businessmen/women when the information is used both for the private and professional spheres of the individual/entrepreneur, such as the tax identifier which is the same number for both spheres by operation of the law. Similarly, the Spanish approach considers an exhaustive list of data on individuals working for legal persons which are deemed “only professional” that does not include powers of attorney granted in his/her favour by the company at hand or the tax identifier that such individual must necessarily use for his/her professional sphere.

**b. Security measures for the same processor of different EU controllers**

The data protection in the global economy must also revisit the concept of “equivalent” protection. For example, if EU data protection rules are deemed equivalent, there is no reason to have several EU controllers of a group imposing to a same processor the specific security measures imposed by the legislation of each of these data exporters, as long as one of them is subject to the regulations of one EU Member State (or of a country, the data protection legislation of which is deemed “adequate”).

In a long term approach, to approve a European standard could be in mind, inspired by the International Standards approved by the so-called Madrid Resolution. However, in the meantime, it makes sense that, if the processor is established in the EU, the security measures shall be those imposed by the data protection regulations of the place of the processor's establishment. On the contrary, if the processor is established outside the EU, the security measures must be those of the data protection regulations of the place of establishment of any of the controllers, to be jointly decided among them.

**c. Security breaches**

We must learn from the US experience of having a number of States regulating differently the notification breaches. Therefore, we should avoid reproducing a nightmare for those obliged to notify that does not ensure any enhancement on privacy. The Directive 2009/136/EC leaves too much freedom to the Member States: again, the EU market cannot grow properly if different regimes coexist in the EU as to who must notify (controllers and/or processors, operating in all sectors or only in a specific certain sector), to whom the notification must be addressed (the DPA and/or the data subjects), and how and when this notification must be made (which are the events triggering the notification obligation, if the notification must be made individually or not, when such notification must take place, etc.), all in addition to the consequences on the one which notifies, in compliance with the legal duty, regarding eventual sanctions being imposed by the relevant DPA.