



European Privacy Officers Forum

Comments on the Review of the European Data Protection Framework

The European Privacy Officers Forum (EPOF), established in 2001, is composed of company data protection compliance officers and internal legal counsel in charge of data protection in Europe. EPOF is a forum that enables members to exchange experiences about European and international data protection compliance. Further, it serves as a platform for Data Protection Authorities to receive input and to directly interact with business representatives. Hunton & Williams provides the secretariat for EPOF.

This paper responds to the European Commission's consultation on its Communication on a comprehensive approach on personal data protection in the European Union (the "**Communication**") launched on 4 November 2010.

INTRODUCTION

As recognised by the European Commission in its Communication, it is very clear that the current data protection framework needs to be modernised, particularly in light of globalisation and new technologies. Indeed the world has changed beyond recognition since the European Data Protection Directive 95/46/EC (the "**Directive**") was written. The framework as currently drafted and implemented raises significant issues that urgently need to be addressed. These issues mainly relate to the practical application of the rules and the extent to which the law places a disproportionate regulatory burden on legitimate and important organisational and business activity. It is the view of EPOF that valuable resources can be better targeted, both by organisations and regulators, on areas where there is actual risk to individual privacy.

This paper is divided into three broad groups of issues, as articulated in turn below and concludes by making specific recommendations.

CHALLENGE 1: Rules that have become disproportionately bureaucratic

NOTIFICATION

In Section 2.2.2 of the Communication, the European Commission recognises that the current requirement to notify data processing activities to the Member States' Data Protection Authorities ("**DPAs**") is cumbersome and does not provide, in itself, any real added value for individuals. The EPOF encourages all efforts by the European Commission to reduce administrative burdens by revising, simplifying and harmonizing the current notification system.

The notification requirement creates considerable practical difficulty in practice, disproportionate to the benefit brought to individuals. The motivation for the system of notification, and the creation of public registers, is transparency of processing. But experience shows that there is very little public interest in the registers, they are infrequently consulted by individuals.

Moreover, in many European countries the process of notification is excessively bureaucratic, requiring very detailed descriptions of data processing, associated data flows, systems and disclosures. Companies have to expend considerable resources, including the utilisation of the services of outside counsel, to complete the necessary paperwork and to liaise with the DPAs. Furthermore, there is a disconnect between the mechanics of the notification process and the dynamic of modern networked companies, which are constantly developing new products and services, and implementing new systems, in meeting the demands of fast moving markets.

The situation is compounded for multi-national companies by the fact that the notification requirements vary from country to country, often quite considerably. For example, in some countries exemptions apply to the processing of employee, client or business contact data, but not in others. Also, the notification procedure and format of the notification form differ from country to country, requiring a different approach for each country. Therefore, even when data processing is very similar within different group companies around Europe, it is difficult to leverage the effort used for a notification in one country to notifications in other countries.

TRANSFERS

The rules regulating personal data exports can be particularly problematic. Articles 25 and 26 of the Directive regulate for a simpler world, where transfers seemingly involve a one-off movement of data between Point A and Point B, between two entities only. The European Commission recognises the general need to improve the current mechanisms allowing for international data transfers in Section 2.4.1 of its Communication. We request the European Commission to take into account the following experiences and observations of EPOF's members in its efforts to improve the current international data transfer framework.

The legal solutions to facilitate data transfers are limited. The list of countries on the European Commission's approved list, although expanding, remains very short, and of limited assistance in practice. The US Safe Harbor can be of significant value to US-based companies (though not all, for instance, the financial services sector is excluded), but does not solve the global problem.

The contractual options have significant drawbacks for complex multi-national companies. Often data transfers involve numerous data exporters on the one side, and data importers on the other. Business operations involving 'onward data transfers' and 'sub-processing' are commonplace in the current business environment. Companies invariably need to set up and manage a myriad of contracts, and update them each time any processing activity changes. This situation is compounded by the fact that a large number of DPAs require that they be notified of data transfers and associated export agreements. Moreover, in certain cases prior permission of the DPA is required for data exports, sometimes even if the model contracts approved by the European Commission are used. Some DPAs take months, even years, to assess permit applications.

The development of Binding Corporate Rules ("**BCRs**") gives multi-national organisations some hope for more flexibility to handle international data transfer restrictions. However, while there is, in theory, a joint procedure for obtaining an approval for BCRs, in practice most DPAs still insist on additional formal applications. In some instances, DPAs require fresh applications for any new processing activity, which substantially undermines the purpose of BCRs. Although improvements to the process have been made and initiatives such as mutual recognition are to be welcomed, putting in place BCRs remains costly and time-consuming. As a result, it is an option only pursued by a few large multi-national companies. Furthermore, the current BCRs

approval process places a heavy burden on DPAs. As increasing numbers of companies opt for this approach, delays can only be expected to get worse and other activities by the DPAs will be negatively affected. Finally, BCRs will only be a truly comprehensive solution when the concept of BCRs is extended to include processing activities by data processors, both within the organisation and by third party suppliers.

SECURITY REQUIREMENTS

In many EU Member States, controllers are required to conform to prescriptive, state-mandated security requirements. Variations in these requirements between Member States imposes an unnecessarily complex burden on multi-national companies, particularly if the same processing activity is subject to different security requirements in different Member States. What's more, prescriptive security requirements encoded in regulation cannot possibly keep pace with advances in the technologies that keep organisations one step ahead of those who attempt to bypass security controls to harm the organisation or individuals whose personal data the organisation processes such as its employees and customers. Regulation cannot possibly keep pace with developments in state-of-the-art security technologies, and it shouldn't try to.

While the Communication is silent on these issues, we urge the European Commission to consider them as part of its simplification and harmonisation efforts.

CHALLENGE 2: Issues raised by legal concepts and definitions

Similar to the way that the notification and data export rules fail to reflect the reality of today's world, many of the legal concepts built into the Directive do not provide effective regulation for modern organisational structures, inter-relationships and processes, again creating unnecessary obstacles to the legitimate processing of personal data.

Controller & processor. The Directive distinguishes between two main actors involved in data processing: the 'controller' as the entity that determines the purposes and means of the data processing, and the 'processor' as the entity that processes data on the instructions and on behalf of the controller. However, the reality of modern day processing is more complex than this simple duality suggests.

The Communication unfortunately does not address these issues. Nonetheless, for the benefit of legal certainty, we strongly encourage the Commission to re-consider the concepts of controller and processor and their inter-relationship in light of the observations set out below.

In practice, the control relationship can be significantly blurred, particularly if multiple parties are involved, for example in a global corporate structure. Our members commonly find that a particular processing operation involves several legal entities each exercising some degree of control, either shared or separate, over the purposes and means of processing. Often there is uncertainty and disagreement between the involved parties as to their responsibilities and liabilities in such case. The uncertainty is increased due to the fact that the concept of joint controllership is not well-defined or acknowledged by European data protection law and local DPAs.

An area where these issues are particularly apparent is outsourcing. While the outsourcing organisation articulates *why* the data is collected and used, the service provider typically determines *how* the data is processed, for example in designing the architecture of information technology platforms or establishing the protocols for a marketing campaign. Who is controller in this scenario and is the service provider merely a processor? The confusion in this area was

perfectly exemplified in the recent high profile case relating to US law enforcement access to financial data held within the SWIFT inter-bank messaging network. SWIFT had been confident that it was operating in the role as a processor. However, there was significant disagreement in Europe between DPAs as to who 'controlled' the data processed on individuals within the network, the banks as customers or SWIFT itself.

Another area which has already created uncertainties due to the lack of clarity around the concepts of controller and processor in light of new Internet data processing models is that arising from privacy and data protection violations through user generated content, where a third party (for instance, an individual) processes information, chooses the means and/or the purposes of the processing using an internet intermediary, such as a web hosting platform. Unlike the cases under the scope of the e-Commerce Directive (2000/31/EC) (including harmonized copyright and defamation liability limitations), the EU data protection framework was not conceived to take these cases into account, nor the liability limitations of internet intermediary providers, irrespective of whether they are controllers jointly with others or processors.

Additional issues arise when sub-processors are used. In today's business environment, large organisations frequently create chains and networks of entities involved in data processing, running from the original controller, through to processor(s), onto a number of sub-processors. The Directive is in this context over-simplified, just catering for a direct relationship between controller and processor. This has led to a number of DPAs holding that there must always be a direct contractual relationship between the controller and each outsourcing service provider 'down the line'. In the context of complex outsourcing arrangements, this can result in an unnecessary burden to put in place and maintain a myriad of agreements between the controller and each outsourcing service provider. A more pragmatic and workable approach is followed by other DPAs, for example in Spain and the UK, which allow for the first processor's obligations to be contractually passed on to sub-processors 'down the line'. This is done on the condition that each sub-processing arrangement is subject to controller consent, and the controller has the power to enforce its rights against any outsourcing service provider involved.

Third party & affiliates. Another concept that the Communication is silent on, but which in practice raises significant interpretational issues, is the definition of 'third party'. Under the present definition each corporate affiliate is considered a 'third party' with regard to every other affiliate. This causes unnecessary compliance issues, especially for larger companies. For example, ensuring a legal basis for data transfer between affiliated companies, in some cases even if the companies are all established within the EU, is unnecessarily burdensome, particularly if the data are non-sensitive in nature, such as business contact details. Moreover, within a corporation the separation of functions does not necessarily coincide with the legal structure of the corporation. For instance, employees working at a company's legal department may be spread over many different legal entities while functionally falling under the same department. Cooperation between these employees, e.g. when they exchange e-mails, should not unnecessarily be restricted by the limits to data transfers imposed by the Directive. The law should provide that groups of companies belonging to the same corporate family are not considered as third parties among themselves. This is an established concept in other areas of law such as competition law, where the parent and each of its subsidiaries are treated as a single economic entity if they form an economic unit within which the subsidiary has no real freedom to determine its own course of action on the market.

*Definition of personal data & identifiability*¹. In its Communication, the Commission promises to examine how to strengthen the principle of data minimisation, *i.e.* the requirement for organisations to limit the processing of data about identified or identifiable individuals to the extent necessary to achieve any particular purpose. In this exercise, the Commission should take into account and promote a subject not addressed in the Communication, namely data anonymisation. Anonymisation of personal data is a process which fundamentally supports the concept of data minimisation, by allowing information about individuals to be processed without reference to identifying features.

A strict interpretation of the notion of “identifiability” has the potential to threaten the advancement of anonymisation as a practical and effective concept to enhance the protection of individuals’ privacy. Personal data is very broadly defined as “any information relating to an identified or identifiable natural person...”. In general terms, a person can be considered as ‘identified’ if they can be ‘distinguished from the group’, and a natural person is ‘identifiable’ when, although the person has not been identified yet, it is possible to do so. If this definition is applied unqualifiedly, it leads to interpretations where data which ostensibly does not relate to natural persons, will be considered ‘personal’ and subject to the full remit of the law if in some way a specific individual may be identifiable. The concept of personal data should rather be defined pragmatically, based upon the likelihood of identification, as per the qualifying principle set out in Recital 26 of the Directive².

Organisations cannot reasonably be expected to guarantee that there is no conceivable method, however far-fetched and even if not pursued in practice, by which the identity of individuals can be established. This is a highly impractical approach, generally requiring excessive resources to be expended on disproportionate statistical analysis. The rights, freedoms, and legitimate interests of individuals can more than adequately be protected if data is processed in such a way that all means which will likely reasonably be used would not lead to identification of said individuals. In particular in this context, it is our contention that ‘coded’ data should typically not be regarded as personal data in the hands of a recipient, where it has no practical or legal means to access the ‘key’ held by a disclosing legal entity (for example clinical trial key coded data in the hands of the sponsor rather than the investigator, or an IP address in the hands of a website operator rather than the ISP). It is also not clear whether the process of anonymisation itself may, absent of an alternative legal basis, require the explicit consent of the individual, given the Directive’s very wide definition of ‘processing’. It should be made clear that the act of anonymisation itself is not subject to the consent and other requirements of the Directive.

Organisations are discouraged from adopting anonymisation as a privacy enhancing technique, when in reality they have to expend disproportionate resource de-identifying data to the required standard, or in seeking unnecessary consents from individuals. De-identification processes established to process data without reference to individual identity, to enhance privacy, particularly found in the health and online sectors, should not be undermined by the blind application of data protection rules that in essence are designed to protect the processing of identifiable personal information. In June of 2007, the Article 29 Working Party (the “**Art. 29 WP**”) published its Opinion on the definition of personal data³. One of the key issues addressed

¹ This issue was discussed in detail in EPOF’s 2006 position paper on the Definition of Personal Data. <http://www.hunton.com/Resources/Sites/general.aspx?id=483>.

² “whereas, to determine whether a person is identifiable, account should be taken of all means likely reasonably to be used either by the controller or by any other person to identify the said person...”

³ Article 29 Working Party, Opinion 4/2007 on the Concept of Personal Data, 20 June 2007. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

by the paper relates to 'identifiability', in particular where the dividing line is drawn between 'personal data' and 'anonymous data'. The paper brings some helpful clarity to the definition of personal data in this context, but the situation is far from being settled on a pragmatic basis, not in the least because, as the paper acknowledges at the end, Member States are largely free to take their own position on these issues, which creates legal uncertainty and unnecessary burdens.

Applicable Law. The EPOF welcomes the European Commission's commitment to revise and clarify the existing provisions on applicable law as set out in Section 2.2.3 of the Communication. The recently published Opinion from the Art. 29 WP on applicable law adopted on 16 December 2010⁴ provides helpful guidance and recommendations, including a proposed shift back to the country-of-origin principle, where the controller applies the local data protection law of the country where its main EEA establishment is located, rather than having to apply different local laws to each individual establishment. We request the Commission to take account of the following observations during its evaluation of the current applicable law provisions.

The current formulation of Article 4 of the Directive causes problems for businesses, since it is very difficult to determine with certainty which national law applies to a particular data processing activity and whether EU law applies at all when the data controller is established outside the EEA; this is especially true for online processing. At the very least, the concept of 'establishment' as used in Article 4(1)(a) should be interpreted uniformly in the Member States. It should not be the case, for example, that some Member States regard every economic activity on their territory, however transitory, as an 'establishment' for the purposes of Article 4 (this is apparently the case in Finland and Sweden, for example). We also prefer a legislative approach in which the law governing the primary relationship between the data controller and the data subject also governs the data flows. Such an approach would centralise the law applicable between the data controller and the individual. For instance, if Dutch law governs the employment contract between a Dutch multinational and an employee in France, why should French law cover the data flows between France and the Netherlands while those data flows are only incidental to the employment relationship?

Further, the application of EU law under Article 4(1)(c) based on the use of 'equipment' should not apply to countries that have been deemed adequate by the European Commission. It seems unnecessary and inappropriate to burden a company which uses equipment in a country that has been deemed adequate with additional application of EU law. For example, if the Swiss data protection legal framework is already deemed 'adequate', why would additional measures meeting the specific legal requirements of one or many EU Member States also be necessary?

The one application of Article 4(1)(c) that is particularly problematic arises when non-EEA established website owners place a cookie on the hard drive of a computer within the EEA. To the extent that personal data (based on real or virtual identity) is processed in respect to this cookie, then many European supervisory authorities will determine that the remote website owner is a controller using 'equipment' within the Community. As the use of cookies is so prevalent on the internet, the logical ramification of this position is that all Member States data protection laws are consistently applicable to all website controllers globally. In a global interconnected online world, cookies are only one example of the impracticability of applying the existing jurisdictional approach, relying on the location of equipment in determining the applicable law.

⁴ Article 29 Working Party, Opinion 8/2010 on applicable law, 16 December 2010.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

CHALLENGE 3: Little assessment of privacy risk and potential harm to the individual

What is absolutely clear to privacy professionals working with European data protection law on a practical everyday basis is that the rules are frequently not designed to reflect the risk to individual privacy in any one situation. The requirements are in most cases prescriptive and applicable to all processing of personal data irrespective of the actual risk to privacy. Such an approach often leads to disproportionate efforts and the use of excessive resources to achieve compliance.

There are some provisions within the Directive which allow for a risk assessment in specific situations. Notably Article 7(f) provides a legal basis for the processing of non-sensitive data where this is “necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject...”. This so called ‘balance of interests’ clause provides a pragmatic alternative to individual consent. This is particularly useful for organisations when processing basic personal information without having direct contact with the potentially vast numbers of data subjects. This typically happens if the organisation collects data from a third party or a public source. If the processing of the data represents no meaningful threat to the interests of the individual, then it may proceed without recourse to lengthy and expensive efforts to gain consent. A key problem here is that a number of Member States, such as Hungary, have not actually implemented Article 7(f) into their law, and in others, such as Germany, it is very narrowly interpreted by the DPAs.

Article 11(2) of the Directive represents a similar pragmatic provision, allowing for an exemption from the requirement to provide a data protection notice to individuals where their personal data are collected indirectly and providing notice would involve a disproportionate effort. As with Article 7(f), this provision is not transposed in a harmonised or pragmatic way across the EEA. In some cases, for example in Italy, a controller actually needs permission of the DPA to rely on this exemption.

Generally, however, the Directive lacks provisions that provide for a more general risk assessment or exemptions in case disproportionate efforts are required to meet the letter of the law. The necessity of gaining consent, or even providing notice, where large amounts of basic non-sensitive data are collected indirectly is questionable. For instance, should the rules on data export be applicable in all cases? What real benefit is gained for personal privacy by applying the same set of rules to business contact data as to consumer data, or applying the strict transfer requirements to a global company’s internal address book? And to the extent that pharmaceutical key coded data is personal in the hands of the sponsor, or an IP address is personal in the hands of a website operator, how necessary or practical is it for those parties to apply all the rules when they do not know who the data subject is? Should the law apply in full to the processing of free text in a business email or meeting report, when an individual is mentioned simply in passing, in circumstances where the content of the communication does not meaningfully relate to that particular person?

The importance of assessing risk in respect to specific data processing operations is increasingly accepted as a fundamental element of an organisation’s approach to personal data protection. DPAs support the use of ‘privacy impact assessments’ for new processing projects that may raise substantive privacy issues. In fact, the Communication specifies in Section 2.2.4 that the Commission will examine whether to make privacy impact assessments mandatory for specific privacy-sensitive cases. In circumstances where potential harm to individuals is identified, then of course appropriate safeguards should be adopted. It seems equally logical,

however, that if a risk assessment, formal or otherwise, can foresee little or no threat to the interests of individuals, organisations should not have to expend excessive resources on adopting measures which are unnecessary.

WHAT FUTURE ACTION IS NEEDED TO MEET THESE CHALLENGES?

The revision of the current data protection framework by the European Commission provides a unique opportunity to modernise the framework, address interpretational issues, increase harmonisation, reduce unnecessary bureaucracy and decrease legal uncertainty to the benefit of industry, DPAs and of course individual data subjects alike. The following are six key recommendations that we urge the Commission to take into account during the revision period:

1. We fully support the intention by the European Commission expressed in Section 2.2.2 of the Communication to simplify and harmonise the current notification system to reduce administrative burdens, to the benefit of both data controllers and DPAs. Notification to a supervisory authority should be limited to basic confirmation of data processing and organisational contact details. There may be some justification for prior notification of the processing of data that are particularly sensitive or where there is a high risk to individuals. A key improvement would be the introduction of a system of pan-European notification, preferably through one “lead” DPA, mutually recognised in all relevant Member States. Also, formally notified data protection officers could take over this responsibility, as in Germany, France, Sweden and the Netherlands. Transparency for the data subjects would be maintained by virtue of the privacy notices which are, in practice, the only reference point for individuals in combination with the more concise details that are notified as proposed above.

2. The improvement of the current data transfer framework, including a more uniform and coherent EU approach, as proposed by the Commission in Section 2.4.1. of the Communication, is of key importance, and we implore the Commission to consider the following recommendations in this regard. There should be no requirement in any Member State for authorisation from or notification to DPAs if mechanisms for export approved by the Commission are used, such as the data transfer model contracts. The European Commission should clarify the “adequacy assessment” procedure and use concerted efforts to increase significantly the number of third countries with adequacy findings. The new data protection framework should also provide for a uniform fast track mutual recognition procedure for the approval of Binding Corporate Rules covering all Member States. An important modernisation would be the introduction of a system of accreditation by appointed and recognised agents/third parties. To reduce the need for frequent contractual amendments as data processing changes, the appendices to the data transfer model contracts, cataloguing information to be transferred and associated purposes, should be made more general in nature.

Other solutions such as ‘BCRs for processors’ and model contracts that can be used by a service provider on behalf of all its clients using a similar service should be included in the revised EU data protection framework. While these proposals would provide greater flexibility for companies and a more manageable approach for DPAs, the interests of data subjects would still be protected. In the case of model contracts, the binding nature of the pre-approved contractual language, the third party beneficiary rights and the other data protection principles such as fair and lawful processing and purpose limitation would ensure that companies could not abuse the solution. In the case of ‘BCRs for processors’, the applicant would demonstrate the effectiveness of their compliance regime to the involved DPA, which could scrutinise the arrangements before and after approval.

3. It is imperative that under the revised EU data protection framework, all Member States be precluded from imposing unharmonised and prescriptive security requirements on controllers. This approach makes pan-European operations unnecessarily complex, and runs counter to best security practices by 'hard coding' requirements into law. In the current information age, organisations need to be able to retain flexibility to swiftly adapt to security threats that potentially harm privacy and public organisations and citizens alike. State-of-the-art should mean state-of-the-art.

4. Key definitions in the Directive should be amended to be more suitable for modern organisational structures, inter-relationships and processes. In particular, the concepts of 'controller' and 'processor' and their inter-relationship clearly needs to be reconsidered. Probably the only practical approach is to make any party processing personal data responsible for compliance, but only to the extent necessary to protect personal data in respect to a particular processing operation, and only to the extent that that party has the legal right to control the data. The concept of "third party" in the context of affiliates within the same corporate structure should also be revised. Furthermore, the definition of personal data should be revised to allow for a more pragmatic approach which promotes rather than discourages anonymisation of data.

5. As recognised by the Commission in Section 2.2.3 of the Communication, the rules on applicable law need to be revised. A possible solution, supported by the Art. 29 WP in its recent Opinion 8/2010 on applicable law, would be the adoption of a "country-of-origin" principle, a principle already well established in other sectors in Europe, for example under the e-Commerce Directive (2000/31/EC).

6. Pursuant to its endeavours to increase harmonisation of data protection law, a key component of the European Commission's strategy set out in the Communication, the Commission should ensure that under the revised EU data protection framework, provisions that allow disapplication of the rules in cases where there is little or no threat to the data subject are properly implemented at a national level, in particular the current Article 7(f) of the Directive. Furthermore, the revised framework should allow for a more pragmatic risk-based approach to compliance by organisations (risk assessed on potential harm to individuals). This will not only mean ongoing support for privacy impact assessments in scenarios of high risk processing, but acknowledgement that legitimate processing, where there is insignificant risk to the interests of individuals, should be allowed without the need to implement safeguards that are disproportionate.

The adoption of the measures that we recommend would clearly provide a positive contribution to a regulatory data protection landscape that respects personal privacy, removes many unnecessary barriers to legitimate data processing by organisations, and will also free up the resources of the DPAs.

We also encourage the European Commission to take account of the 'accountability model', which has been most closely associated with the ongoing work of the Centre for Information Policy Leadership in the context of its 'Galway project'.⁵ The accountability model envisages a regulatory environment that is far less based on prescriptive administrative procedures, but rather creates mechanisms to provide confidence that organisations processing personal information can be relied upon to ensure defined and accepted privacy outcomes if they are effectively held to account. For a more detailed description of the accountability model, we refer to EPOF's previous submission and to the resources available on the Center for Information

⁵ <http://www.hunton.com/Resources/Sites/general.aspx?id=965>.

Policy's website.⁶ Also, the Art. 29 WP has recently published an opinion on the principle of accountability.⁷

For any question about this paper, please contact the EPOF Secretariat:

Christopher Kuner
Hunton & Williams
Park Atrium
Rue des Colonies 11
B-1000 Brussels
Phone: +32 2 643 5856
E-mail: ckuner@hunton.com

* * *

⁶ <http://www.hunton.com/Resources/Sites/general.aspx?id=45>.

⁷ Article 29 Working Party, Opinion 3/2010 on the Principle of Accountability, 13 July 2010.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.