



# European Privacy Officers Forum

## Comments on the Review of European Data Protection Framework

The European Privacy Officers Forum (EPOF), established in 2001, is composed of data protection compliance officers and internal legal counsel in charge of data protection in Europe from approximately forty multi-national companies. EPOF members deal with issues raised by the practical implementation of European data protection law on a daily basis. This paper forms a submission to the European Commission consultation on the legal framework for the fundamental right to protection of personal data, launched on 9 July 2009. EPOF members feel that it can uniquely articulate on the practical challenges for personal data protection from the perspective of large commercial organisations conscientiously seeking to implement the law and best practice on a pan-European and global basis. This submission has been drafted jointly by the members of EPOF.

### EXECUTIVE SUMMARY

The European Data Protection Directive provides the foundation of an established legal framework, based upon internationally agreed principles, that are of significant benefit to individuals and to society as a whole. However, the dynamic and complex information society of the 21st Century requires a regulatory regime that is effective in meeting the challenges presented to organisations processing personal information and addresses actual risk to individuals. The significant issues raised by the current regime, mostly regarding practical application and disproportionate regulatory or bureaucratic burden, must evolve to recognise and take advantage of the opportunities presented by globalisation and new technology.

#### The Challenges:

##### 1 - Rules that have become disproportionately bureaucratic

*Notification* represents an excessively bureaucratic process, varying from country to country in format, requiring considerable resource to manage, disproportionate to the benefit brought to individuals.

*Transfers* in today's dynamic and globalised information society are governed by data export rules developed for a simpler world. The new situation requires legal solutions that address the complex and global nature of data flows.

##### 2 – Issues raised by legal concepts and definitions

*Controller and Processor.* The definitions of these central concepts do not reflect the reality of the complex control relationships that govern the handling of personal information in today's world, creating confusion and unnecessary obstacles to the legitimate processing of personal data.

*Third party and affiliates.* The definition of these concepts present problems when providing a legal basis for data sharing among a group of companies where the separation of functions does not necessarily coincide with the legal structure.

*Definition of personal data.* The concept of personal data should be defined pragmatically, based on the likelihood of identification, to encourage organisations to anonymise personal information wherever possible, and to facilitate the processing of data about de-identified individuals for purposes of considerable benefit to society as a whole.

*Applicable law.* The current rules determining the law applicable to the processing of personal data in any one case make it difficult to determine which jurisdiction's legalisation applies, especially when a controller is located outside the European Union, or the processing takes place online.

### **3 – Little assessment of privacy risk and potential harm to the individual**

*Risk assessment* should be considered fundamental to an organisation's approach to personal data protection. There should be more widespread use of 'balance of interests' as a pragmatic alternative legal basis to consent for less sensitive data processing.

#### **What future action is needed to meet these challenges?**

Much can be achieved by a more pragmatic interpretation of the data protection legal framework, of benefit to both organisations and individuals, in the following areas: (1) notification; (2) data exports; (3) prescribed security requirements; (4) key definitions; (5) applicable law; (6) risk assessment. The Commission should also consider an innovative approach to personal data protection based upon the accountability of organisations.

## **INTRODUCTION**

There is no doubt that there are inherent strengths in the established legal framework for data protection within the Community, which are of significant benefit to individuals and to society as a whole. In particular, the principles that form the foundation of the European Data Protection Directive 95/46/EC ("Directive") have a central role in safeguarding personal information and providing important rights to individuals. Purpose specification, collection limitation, transparency, data integrity, information security, access and correction are examples of key principles not only present in the Directive, but in other international data protection instruments such as the OECD Guidelines<sup>1</sup>, the Council of Europe Convention<sup>2</sup> and the more recent APEC Privacy Framework<sup>3</sup>. The Directive has also helped harmonise data protection rules across Europe, assisting to a large degree in the creation of an internal market for personal data. The legislation is to a large extent technology neutral, and there is no doubt that European citizens are now more aware of data protection issues and their informational rights.

It is very clear however that European data protection law as currently drafted and implemented raises significant issues that urgently need to be addressed. These issues in the main 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

<sup>1</sup> OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980. [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html)

<sup>2</sup> Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

<sup>3</sup> Asia-Pacific Economic Cooperation (APEC) Privacy Framework. [http://www.apec.org/apec/apec\\_groups/committee\\_on\\_trade/electronic\\_commerce.html](http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html)

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.

The Commission consultation is in particular seeking opinions on *new* challenges for personal data protection, particularly in the light of new technology and globalisation. Whilst some of these difficulties are ongoing rather than new, the degree to which they represent a challenge becomes yet more apparent as modern society becomes increasingly complex technologically and economies become more networked and global in nature. Indeed the world has changed beyond recognition since the Directive was written. The modern globalised information-based economy is now incredibly dynamic. Multi-national companies are increasingly networked, deploying centralised hubs to increase economies of scale, utilising sophisticated offshoring operations in the developing world. At the same time, business operations are increasingly global in nature, meeting the needs of customers around the clock, developing solutions for clients whose own services are more global in nature. Such processing operations may require access to centrally held data by a number of business units globally, perhaps simultaneously. Cloud computing is increasingly prevalent, in which dynamically scalable and virtualised resources are provided as a service over the Internet. An inherent characteristic of cloud computing is the dynamic and multi-locational nature of server hosting.

All these trends have laid bare some of the deficiencies of the current system and have magnified the challenges which the current regulatory framework presents. These challenges, divided into three broad groups of issues, are articulated below. The paper concludes by making recommendations, and describing an alternative approach to data protection that we feel would improve the safeguards afforded to individuals' information, better suited to the modern world.

### **CHALLENGE 1: Rules that have become disproportionately bureaucratic**

#### *NOTIFICATION*

The requirement to notify data processing to supervisory data protection authorities can create considerable practical difficulty, disproportionate to the benefit brought to individuals. The motivation for the system of notification, and the creation of public registers, is transparency of processing, so individuals can see what personal data an organisation is handling and the associated uses and disclosures. But, experience shows that there is very little public interest in the registers, they are infrequently consulted by individuals.

At the same time, 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 often have to expend considerable resource, including the utilisation of the services of outside counsel, to complete the necessary paperwork and to liaise with the supervisory authority. 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 requirements for notification vary from country to country, often quite considerably. In some countries exemptions apply, for example relating to the processing of employee, client or business contact data, but not in others. In some jurisdictions prior approval is actually required to use European Commission model contract clauses. Even when data processing is very similar within different group companies around Europe, it is difficult to leverage the effort expended for a notification in one country in order to notify in another country, because the format of the documentation requires a different response in each case.

## *TRANSFERS*

The rules regulating personal data exports can be particularly problematic. Articles 25 & 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 just two entities. The legal solutions to facilitate data transfers are limited. The list of countries that appear on the European Commission's approved list remains very short, and of little practical assistance. 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 option has significant drawbacks for complex multi-national companies. It is quite possible that each data transfer will involve numerous data exporters on the one side, and large numbers of data importers on the other. Business operations involving 'onward transfer' and 'sub-processing' are commonplace. A myriad of contracts invariably needs to be raised and managed. Of course, as soon as data processing changes, perhaps with new data or a new purpose, the myriad of agreements need to be amended. This situation is compounded by the fact that a large number of Data Protection Authorities ("DPAs") require that they be notified of data transfers and associated export agreements and in certain cases, permission is required before processing can begin. In some cases, this even applies in respect to the model agreements approved by the European Commission, the regulators being interested in the appendices outlining the proposed data processing. Some regulators can take months, even years, to assess these applications. There are also indications that certain DPAs are actually disallowing use of the model agreements in certain circumstances, for example, the Controller to Controller clauses for the outsourcing of direct marketing activities within groups of companies.

Of course, the development of Binding Corporate Rules ("BCR") provides some hope for multi-national organisations of a more flexible regulatory regime for data exports. It is at face value an attractive idea, that a system of internal corporate governance covering the processing of personal data within a multi-national group of companies can be assessed in advance as providing adequate protection for exported personal data. However, whilst there is, in theory, a joint procedure for obtaining an approval for BCR, most regulators still insist on additional formal applications and, in some instances, they require fresh applications for any new processing which undermines substantially the purpose of BCR. The process has become shorter and initiatives such as mutual recognition are to be welcomed, but it does remain costly and relatively lengthy, an option only chosen so far by a few multi-nationals. The burden on DPAs presented by the current BCR process is also recognised, and as increasing numbers of companies opt for this approach, associated delays can only be expected to get worse. Of course, only when the concept of BCR is extended to an applicant's data processing activities in its capacity as a processor as well as the processing carried out on its behalf by its suppliers will BCR be heralded as a truly comprehensive solution.

## *SECURITY REQUIREMENTS*

In eight EU Member States, plus one European Economic Area country, controllers are required to conform to prescriptive, state-mandated security requirements. Variations in these requirements between Member States create an unnecessarily complex burden on multi-national companies. What's more, prescriptive security requirements encoded in regulation cannot possibly keep pace with advances in the technologies that keep companies one step ahead of those who would bypass security controls to do harm to them and their customers. Regulation cannot possibly keep pace with developments in state-of-the-art security technologies, and it shouldn't try to.

## **CHALLENGE 2: Issues raised by legal concepts and definitions**

Similar to the way that the rules on Notification and data export fail to reflect the reality of the 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 identifies two types of organisation as being involved in the processing of personal data. A 'controller' is defined as the party that determines the purposes and means (the 'why and how') of processing personal data and is liable for the correct handling of that data. A 'processor' handles personal information under contract to the controller, operating under instruction and applying appropriate security safeguards. However, the reality of modern data processing is more complex than this simple duality suggests.

In a whole variety of settings, the control relationship can be significantly blurred, not least if multiple parties are involved. Frequently our members find that a particular processing operation can involve two or more legal entities each exercising some control over the purposes and means. There is often disagreement between the different parties on their responsibilities and liabilities in this case. This is not helped by the fact that the concept of joint controller is not well acknowledged by European data protection law and supervisory authorities. In respect to outsourcing, it is often the case that the appointed party determines *how* personal data is processed, for example in designing the architecture of information technology platforms or establishing the protocols for a marketing campaign, whilst the party contracting these services articulates *why* the data is collected and used. Who is controller in this context? 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 messaging network. SWIFT had been confident that it was operating in the role as a processor. However, there was significant disagreement in Europe between data protection authorities as to who 'controls' the data processed on individuals within the network, the banks as customers or SWIFT themselves. Large multi-national organisations struggle in handling these concepts, so it is possible to imagine the difficulties for small and medium sized enterprises.

An additional issue arises from the fact that processors often appoint sub-processors. Experience shows, with multi-national companies, that frequently chains and networks of stakeholders can be created, running from the original controller, through to the processor, 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 interpreting the law so that there always has to be a direct contractual relationship between the controller and each outsourcing party 'down the line'. Of course, in the context of complex outsourcing arrangements, this can result in a myriad of agreements between the controller and each outsourcer. However, one or two DPAs, including those from Spain and the UK allow for the obligations of the first processor to be contractually passed on to sub-processors 'down the line', consistent with the standard contractual approach adopted for other legal purposes. 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 outsourcer. This is a much more pragmatic approach.

*Third Party & Affiliates.* The present definition of 'third party' causes problems for companies in many Member States, since each corporate affiliate is considered a 'third party' with regard to every other affiliate, meaning that they must ensure there is a legal basis for data transfer even among a group of companies, and in some instances even if the companies are all established within the EU. Moreover, within a corporation the separation of functions does not necessarily coincide with the legal structure of the corporation. For instance, a

company legal department may be spread over many different legal entities while still being functionally the same department, in which people should be able to work together without taking into account the limits to data transfer contained in the Directive. The law should ensure that groups of companies belonging to the same corporate family are not considered as third parties among themselves. This is a concept found in other areas of law such as competition law, where even if the parent and subsidiary have distinct legal personalities, if they form an economic unit within which the subsidiary has no real freedom to determine its course of action on the market, they are treated as a single economic entity.

*Definition of Personal Data & Identifiability*<sup>4</sup>. The concept of 'data minimisation', the requirement for organisations only to process data about identified or identifiable individuals where absolutely necessary for any particular purpose, is a fundamental principle of data protection. The anonymisation of personal information is a process which fundamentally supports this concept, allowing information about individuals to be processed without reference to identifying features. Organisations that process personal information should be encouraged to anonymise wherever possible. However, in Europe a strict interpretation of data protection law has the potential to threaten the advancement of anonymisation as a practical concept. Personal data is very broadly defined in Article 2 of the Directive 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. Where the Article 2 definition is applied unqualifiedly, then it may be interpreted in such a way that data, ostensibly not about natural persons, will be considered 'personal' and subject to the full remit of the law if specific individuals are *in any way* identifiable.

The concept of personal data should rather be defined pragmatically, based upon the likelihood of identification, as per the qualifying principle present in Recital 26 of the Directive<sup>5</sup>. It should not be the case that an organisation has to be sure that there is no conceivable method, however unlikely in reality, by which the identity of individuals can be established. This is a highly impractical approach, usually requiring considerable resource 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 *likely reasonably* to be used to identify the said person will fail. 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 organisation, where they have 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 may also be the case that the process of anonymisation itself may, absent of an alternative legal basis, require the explicit consent of the individual has to be sought. This is because the concept of 'processing' under the Data Protection Directive is very widely defined. Although it may not have been the intention of those drafting the legislation, it is conceivable that this definition catches all conceivable processing activities, including the act of anonymisation itself.

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-

---

<sup>4</sup> 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>

<sup>5</sup> "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..."

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 published its long awaited Opinion on the definition of personal data<sup>6</sup>. One of the key issues addressed 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.

*Applicable Law.* The current formulation of Article 4 causes problems for business, since it is very difficult to determine with certainty which national law applies to a particular act of data processing and whether EU law applies at all when the data controller is established outside the Community; this is especially true when the processing is online. The concept of 'establishment' as it is 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, however transitory, on their territory 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 Commission. Indeed, insofar as these countries have in place legal frameworks that would cover the data processing in a way that the Commission has deemed adequate, it seems inappropriate to burden such companies with the 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 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 inter-connected 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.

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

What is absolutely clear to privacy professionals in 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

---

<sup>6</sup> Article 29 Working Party, Opinion 4/2007 on the Concept of Personal Data, 20 June 2007. [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2007\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm)

prescriptive and applicable to *all* processing of personal data. Such an approach often leads to disproportionate effort in terms of the amount of resource expended on compliance.

There is some provision within the Directive for an assessment of risk 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 at Article 7(a) as a criterion for making processing legitimate. This is particularly useful for organisations in circumstances where basic personal information is to be processed, but the data subjects themselves (and there may be large numbers of them) are not directly in contact. This typically may happen if data arrives via a third party or is collected from 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. The difficulty here is that a number of Member States have not actually implemented 7(f) into their law (such as Hungary) and in those countries that have the provision it is very narrowly interpreted by supervisory authorities (for example in Germany). A similar pragmatic provision is represented by Article 11(2) of the Directive, allowing an exemption from the requirement to provide a data protection notice to individuals where their personal information is collected indirectly and to provide the said notice would involve a disproportionate effort. This exemption is to apply particularly for statistical, scientific and historic processing, but not exclusively in relation to those purposes. As with 7(f), this provision is not transposed in a harmonised or pragmatic way across the Community. In some cases, for example in Italy, a controller actually needs the permission of the supervisory authority to use the provision.

Generally however, the Directive is missing provisions that provide for a more general assessment of risk or harm when processing of personal data occurs, allowing for wider exemption of the law’s requirements on the basis of disproportionate effort. The necessity of gaining consent, or even providing notice, where large amounts of basic non-sensitive data are collected indirectly is questionable as suggested above. Should the rules on data export be applicable in all cases? For example, 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? 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? How justifiable is it that an organisation has to process a subject access request, maybe expending considerable resource in searching electronic back up systems, without recourse to legal relief on the basis of disproportionality? 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 fundamental part of an organisation’s approach to personal data protection. Supervisory authorities support the use of ‘privacy impact assessments’ for new processing projects that may raise substantive privacy issues. In circumstances where potential harm to individuals is identified, then of course appropriate safeguards should be adopted. It seems equally logical 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 resource on adopting measures which are unnecessary.

## WHAT FUTURE ACTION IS NEEDED TO MEET THESE CHALLENGES?

It is undoubtedly the case that much can be achieved in terms of more pragmatic interpretation and greater harmonisation, perhaps coupled with legislative changes, to the benefit of industry, DPAs and of course individual data subjects. The following are six key recommendations in this context:

1. Notification to a supervisory authority should be limited to basic confirmation of data processing and organisational contact details. There is maybe some justification for prior notification of the processing of particularly sensitive data or generally where there is high risk to individuals. One improvement could be to introduce a system of pan-European notification, perhaps through a lead authority, mutually recognised in all relevant Member States. Alternatively, 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 and the more concise details that are notified as proposed above.
2. Responsibility for ensuring adequate protection for personal data exported from the EEA should be in the hands of the exporter with no requirement for authorisation or notification to supervisory authorities if approved mechanisms for export are used (e.g. model clauses). This should be coupled with a concerted effort by the Commission to increase significantly the number of third countries with adequacy findings and a fast track mutual recognition procedure covering all Member States for the approval of Binding Corporate Rules. This procedure could be enhanced by recognising accreditation by appointed third parties. Appendices to data export agreements, cataloguing information to be transferred and associated purposes, should be made more general in nature, alleviating the requirement for frequent contractual amendments as data processing changes. Solutions such as 'BCR for processors' or model clauses that can be used by a service provider on behalf of all its clients using a similar service should be developed as soon as possible.

Whilst these proposals would provide greater flexibility for companies and a more realistic approach for regulators, the interests of data subjects would still be protected. In the case of model clauses, 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 or purpose limitation would ensure that companies could not abuse the solution. In the case of 'BCR for processors' the applicant would demonstrate the effectiveness of their compliance regime to regulators, who would of course be free to scrutinise the arrangements before and after approval.

3. It is imperative that Member States be precluded from imposing unharmonised and prescriptive security requirements on controllers. This approach makes pan-European operations unnecessarily complex, and is counter to best security practice by 'hard coding' requirements into law. 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 definitions of 'controller' and 'processor' clearly need attention. Probably the only practical approach is to make any party processing personal data liable for compliance with the rules, but only to the extent necessary to safeguard personal information in respect to a particular processing operation, and to the extent of that person's legal right to control the data. The definition of personal data should also be

drafted on a more pragmatic basis. It should be possible in this context to match the level of regulation with the degree of identifiability of data.

5. The rules on applicable law should be reviewed. A possible solution could lie in adoption of a system of home country regulation (within the Community), already well established in other sectors in Europe such as electronic commerce. In a recent article, Francis Aldhouse, the former UK Deputy Information Commissioner, makes the case for this more rational system: "Applying their experience since 1995, national data protection authorities have, through the Article 29 Working Party and other means, generated a greater consensus on the application of the law. With increased understanding and confidence between national governments and regulators, the time is now right to amend the Directive, and adopt the practice of home-country regulation. This system of mutual recognition, which is well precedented in the European Union, would allow users of personal information operating in more than one European state to be subject only to the law and regulation of one of those states. Those providing information services from outside Europe in more than one European State would similarly be subject to the jurisdiction of a single European regulator. None of these changes would prejudice the rights of individuals to secure a remedy in their home jurisdiction."<sup>7</sup>
6. Pursuant to its endeavours to create greater harmonisation in implementation of data protection law, the European Commission should ensure that existing provisions within the Directive that facilitate disapplication of the rules in cases where there is little or no threat to the data subject are properly implemented at national level, in particular Article 7(f). Furthermore, supervisory authorities should endeavour to interpret the existing rules so as to support a 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 to proceed without the need to implement safeguards that are disproportionate in nature.

The adoption of the measures that we recommend would clearly lead to a regulatory landscape for data protection that respects personal privacy, removes many unnecessary barriers to legitimate data processing by organisations and will also free up the resources of the data protection authorities. However, increasing numbers of commentators are arguing that an approach more deeply embedded in corporate and information governance is required if we are to 'square the circle', to have an effective regulatory regime for personal data protection within the hugely dynamic information society of the 21<sup>st</sup> Century. A credible, and possibly more effective approach, often referred to as the 'accountability model', has recently been gaining momentum. It has been most closely associated with the ongoing work of the Centre for Information Policy Leadership in the context of their 'Galway project'<sup>8</sup>.

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. The model is in the main based upon internationally agreed general privacy principles, the ones that already form the foundation of the Directive, which we discussed at the beginning of this paper. Industry specific Codes of Practice will play a greater role in specifying how the rules should be implemented in particular settings. Risk assessment also plays an important part in the

---

<sup>7</sup> Francis Aldhouse, "European Data Protection Directive Review", Data Protection Law & Policy", October 2009.

<sup>8</sup> [http://www.hunton.com/news/news.aspx?gen\\_H4ID=16678](http://www.hunton.com/news/news.aspx?gen_H4ID=16678)

accountability model. Organisations must assess the potential harm to individuals from the data processing operations they implement. It is then up to each organisation to design and demonstratively implement a system of informational governance, including privacy impact assessments, policies and procedures, to ensure effective safeguards for individuals. These are supported with training and education for all relevant staff. Privacy enhancing technology should be developed and used as widely as possible to assist the accountable organisation meet its objectives.

The fundamental characteristic of the model is of course that the organisation must be truly accountable. The compliance regime developed, and ongoing performance, must be approved at the highest level within the organisation, ideally signed off annually, similar to a company's accounts. An organisation must additionally demonstrate their commitment by tasking appropriate staff with implementing the privacy programme, headed by a senior officer that will have sufficient authority to ensure compliance. Effective monitoring and audit mechanisms must be put in place to ensure that the privacy programme is working correctly, both within the organisation and with contracted outsourcers. Another characteristic feature of the model is the importance of external verification of compliance and accountability by an independent entity. Such checks can be made by the internal audit departments of other group companies, third-party accountability agents and privacy enforcement agencies. External verification must be both trustworthy and affordable.

There must be an effective means for remediation where harm is caused to individuals by the failure of internal policies and procedures. This should be founded upon a clear and publicised complaints handling mechanism. The organisation may also wish to engage the services of an outside remediation service to assist in redressing complaints. A system of co-regulation can be envisaged where industry associations can take action against companies for breaches of Codes of Practice. What is crucial is that accountability practices should be ultimately subject to effective legal actions by an appropriate enforcement authority. The nature of this authority will likely vary across jurisdictions globally, but will always have effective oversight powers and the ability to impose strong sanctions, both administrative and criminal, against those that wilfully and carelessly misuse personal data.

Of course many elements in the accountability model are recognisable within the concept of Binding Corporate Rules and it is possible that the learning that is being gained by large companies in implementing BCR will assist in the development of the 'accountable organisation'.

EPOF members understand that the accountability model is far from complete as an alternative approach to personal data protection, but are interested in the development of the concept as it seems potentially the only long term solution for privacy in our ever more dynamic information society. We recommend that the European Commission seriously considers this methodology as part of its review process.

## **CONCLUSION**

EPOF represents a group of multi-national companies that have taken the lead in positively seeking to comply with data protection laws and regulations on a pan-European basis. We contend that significant issues are raised as a consequence of the current regime for personal data protection within the Community, both to the detriment of personal privacy and legitimate organisational interests. EPOF is hopeful that the European Commission will seriously consider the recommendations of this paper, because they reflect the practical experience of organisations committed to personal privacy, and welcomes any future collaboration and engagement opportunities with the European Commission in the context of this review process.

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

\* \* \*

*The European Privacy Officers Forum (EPOF) 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. EPOF meets three times a year in Brussels, Belgium. Hunton & Williams provides the secretariat for EPOF.*

\* \* \*