

EPOF

European Privacy Officers Forum

Comments on Review of the EU Data Protection Directive **(Directive 95/46/EC)**

July 31, 2002

The European Privacy Officers' Forum (EPOF)* is composed of data protection compliance officers and internal legal counsel in charge of data protection in Europe from approximately twenty-five companies. As such, EPOF members deal on a daily basis with the compliance challenges presented by the EU Data Protection Directive, and welcome this opportunity to comment to the European Commission on its implementation. While EPOF members are all data protection professionals who strongly believe that an adequate level of data protection is necessary, we also find that substantial problems currently exist regarding implementation of the Directive.

I. INTRODUCTION

The EPOF recognizes that there are a number of ways forward following review of the Directive. These include: (a) a major revision of the Directive; (b) a minor revision; (c) enhanced coordination of national approaches at European level to overcome continuing barriers to the internal market; (d) additional specific Directives; and (e) maintenance of the status quo.

As the following general and specific comments highlight, the EPOF is not suggesting that the Commission should undertake a major revision of the Directive. Rather, we suggest that the Commission reconsider various provisions of the Directive, the application of which leads to unsatisfactory results. This solution would deal with problems faced by industry, while at the same time maintaining the same level of protection for data subjects.

In addition, the EPOF suggests that the Commission take a stricter approach with Member States that do not implement properly certain provisions in the Directive. For example, the Commission should ensure that Member States do not impose prior *de facto* authorization requirements for the transfer of data to countries deemed by the Commission to provide adequate protection.

* Some of the members include Accenture; DoubleClick International TechSolutions Ltd; EDS; Hewlett-Packard; IBM; Intel; Philips; Procter & Gamble; Sun Microsystems; and Yahoo! Europe.

II. GENERAL COMMENTS

A. Need for a harmonised framework at the EU level and more consistency between Member States

Member States have implemented the Directive in very diverse ways. Many Member States have gone far beyond the terms of the Directive in implementing it into national laws. Others have interpreted it in ways that seem to contravene the Directive, whereas others have failed to amend their laws sufficiently to reflect the possibilities of the Directive. We hope that the report on implementation will reflect these hindrances to rapid and efficient data flows, and that the Commission will become more active in limiting such national divergences in order to reach the initial objective, which is to facilitate the functioning of the internal market while at the same time ensuring a minimum level of protection throughout the EU. National divergences jeopardize the goal of the Directive to enable a free flow of data within the Community.

B. Interaction of different pieces of legislation

It is becoming increasingly difficult to deal with the interaction of the various legislative acts such as the General Directive, the E-Commerce Directive, the Electronic Communications Data Protection Directive, the Distance Selling Directive, etc., all of which deal with data protection issues. There should be a single directive dealing with data protection, rather than multiple sectoral provisions, since existing EU sector-specific legislation has created distortions and inconsistencies in the performance of virtually identical business operations among industries.

C. Need for a dialogue on emerging issues

Regulators have often taken reactive responses to new technologies and potential issues (for example, the cookies issue). We would like to see a dialogue established between national data protection commissioners and industry in order to enhance mutual understanding, help encourage proportionate and timely responses to emerging issues, and find acceptable balances between privacy protection and business needs.

D. Multinational companies and personal data

Multinational companies should be allowed to develop unified systems for human resource and customer data management, no matter where the processing of data in such systems takes place, without having excessive obligations imposed on them that go beyond ensuring an “adequate level of protection”.

III. DETAILED COMMENTS

A. Definitions (Article 2) and Exemptions (Article 3)

1. Necessity for a distinction between “personal data” and “professional data” and the need to focus on harm to data subjects

Problems are caused in practice by the fact that the Directive and Member State laws cover the data of individuals in their work capacity as well as in their personal capacity.

For example, if an employee of Company Y receives a business card from an individual who works for Company X and who wants to stay in touch with Company Y for future business opportunities or to receive business-related information, and proceeds to copy the data into an electronic database that contains the names and business addresses of other people gathered in the same way, the database falls within the scope of application of the Directive and all the obligations set forth by the Directive apply to it. The Company Y employee should then inform the individual in writing that his/her details are in such a database, in certain circumstances give him/her the option to have these details removed from the database, and inform him/her how to exercise his/her privacy rights, etc. In some countries, the data controller should also notify the database to the authorities. If Company Y decided to make available the data to an affiliate, in many Member States (such as Spain) it is obligated to obtain unambiguous consent from the individual concerned. Finally, if the data flow changes (because, for example, a new affiliate in a country whose laws do not ensure an adequate level of protection is given access to the data), both the notices and the notifications have to be repeated, although the professional purposes of the data processing are still the same.

While individuals certainly expect a right to privacy with respect to factors specific to their physical, physiological, mental, economic, cultural or social identity, do they expect that information such as that described above should be subject to data protection legislation in the same manner as data related to their personal life? Are an individual's privacy rights at issue when he drafts a report on a company meeting he has chaired, or when he sends his superior an e-mail saying that the negotiations on a particular business transaction are not going well? We suggest that the answer to these questions is “no,” since the sole point at issue is the fact that the individual represents the legal entity that is conducting business, and information is recorded relating to the actions or activities of the individual solely in that context. More importantly, if such data is used within the business purposes for which it was initially collected, the processing of such data causes no threat to the individual's right of privacy. In such a case, the data is only incidentally “personal”, i.e., it really concerns the individual in his business capacity rather than in his personal capacity.

Thus, a Directive designed to protect “fundamental rights and freedoms” should be limited in scope to the recognition of rights that are essential and specific to the

individual as a human being. This could be reflected in an appropriate change to the definition of personal data in the Directive; such a change could involve addition of the following language to Article 2(a) (amended language in boldface):

“‘personal data’ shall mean any information relating to an identified or identifiable natural person ('data subject'), **apart from information relating to a natural person in their work capacity...**”

Alternatively, a new definition conceptualising information relating to work or professional life (perhaps termed ‘professional information’) could be added to Article 2, the processing of which could then be subject to derogations under the Directive. Such a definition could read as follows:

“Information specific to the employment, business or professional responsibilities of a data subject, such as: name, job title, workplace contact details, description of activities and transactions in which he has engaged in order to carry out those responsibilities, reports and other work products, and where they are processed for work related purposes.”

It would also be helpful to achieve consistency among Member States on the question of whether data protection law should cover the personal data of legal persons as well as that of natural persons. The fact that four Member States (Austria, Denmark, Italy and Luxembourg) protect the personal data of legal persons in their data protection laws while the rest do not causes substantial problems for companies operating in Europe. There should be consistency among Member States on the question of whether data of legal persons fall in the scope of the Directive. It would be preferable to limit the scope of data protection in the internal market to natural persons.

2. *Anonymous data*

Anonymisation forms the basis of many innovative privacy-enhancing technologies in the health, Internet and other sectors, and many organisations process anonymised data for the purposes of legitimate and valuable scientific and market research.

The Directive gives some guidance as to the concept of anonymous data in Recital 26: “Whereas, to determine whether a person is identifiable, account should be taken of all the means **likely reasonably** to be used either by the controller or by any other person to identify the said person” (emphasis added).

The problem encountered by companies today is that some Member States overlook the “reasonableness” test set forth by Recital 26. Rather, some authorities have interpreted this to mean that if someone *can* be identified from certain data, no matter how technically or legally difficult it is to ascertain the identity of the physical person from such data, then the data is deemed to be “personal data.” In our view, it should not be the case that to anonymise personal information, an organisation has to be sure that there is

no conceivable method, however unlikely in reality, by which the identity of individuals can be re-established. This is a highly impractical approach, and may actually discourage companies from anonymising data.

We suggest solving this problem by including a new definition of anonymous data in the Directive. The definition should be pragmatic and it should emphasise that the capability of identification must be subject to the reasonableness standard. For example, a definition such as that given in §3(6) of the German Federal Data Protection Act could be satisfactory:

“Depersonalisation means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual.”

A second problem regarding anonymisation is that under some national laws it may be the case that to render personal information anonymous, the explicit consent of the individual has to be sought (for sensitive personal data), or notice of processing has to be provided to that person (personal data), since the definition of “processing” may be defined to include the act of anonymisation itself. To take a practical example, assume that a software supplier wishes to develop a new prescription dispensing system for community pharmacies. A community pharmacist agrees to help with the development and testing of the system, and is asked to provide an anonymised sample data set for testing purposes. The pharmacist strips all features relating to the patient and doctor, and only the data on the drugs prescribed is sent to the software supplier. The software supplier uses the data supplied by adding unrelated pseudonyms. A strict interpretation of the Directive would require that individual patient consent be sought for the anonymisation, and that every doctor whose prescription had been dispensed by the pharmacy would need to be notified, which would be very difficult to achieve in practice.

Thus, there is no purpose in having the definition of “processing” actually cover the act of anonymisation. To alleviate the current legal uncertainty in this area, it would be preferable if Article 2 indicated that anonymisation is a technique specifically excluded from the scope of ‘processing’. Alternatively, if the definition of ‘processing’ in Article 2(b) is to retain its current very wide application, then appropriate pragmatic exemptions from certain key principles of the legislation should be drafted to encourage data controllers to anonymise wherever possible.

3. *Consent*

There is no common approach to consent in the Member States. For instance, in some Member States opt-out involves physical deletion from a company database, while in others it involves just “flagging” the program from which the consumer has opted out. The current situation is difficult to cope with in countries like Portugal, where “flagging”

is not permitted as long as the person has not enrolled on the Robinson List. The result is that when purchasing lists from external sources, companies have no way of knowing whether or not they are sending communications to consumers who have previously opted out.

In addition, in countries that have an opt in regime, the areas for which this opt in is needed are handled differently. For example, in Italy written consent from job applicants for the processing of their applications is needed, whereas the rule is different in other cases.

It would be better to have a European approach that maximises consumer choice and allows consumers to decide specifically what they are “opting out” of or “opting in” for (*e.g.*, receiving all marketing information, or receiving just a particular program, a particular brand, etc.).

4. Definition of “third party” as it relates to 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 in the EU. The Directive 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. This would allow a subsidiary established in Spain to send human resources data to the parent company established in Germany without obtaining consent from the data subjects.

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.

5. Definition of “data controller” and “data processor”

In interpreting the definition of data controller and data processor, the current approach of some data protection authorities is to give a very limited or narrow interpretation to the definition of data processor. In their view, this latter term only applies to those third parties that provide very limited processing functions. This is particularly troublesome for companies that provide sophisticated service models, particularly in the area of technical solutions or services, such as for example,

authentication services, advertisement services, customer relationship management (CRM) systems, etc. In these cases, the service company may set up parameters for the product in advance. The product or service will ultimately be used by each particular customer. However, many data protection authorities would deem such companies to be “data controllers.”

B. Applicable law (Article 4)

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 done on-line.

The following are some suggestions for revision of Article 4:

- 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 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 centralize the law applicable between the data controller and the data subject. 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?
- 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 deemed “adequate” 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. In other words, why should the laws of the fifteen Member States apply to a Swiss company that processes data using equipment (such as cookies) in the Member States, if Swiss law governs this processing and affords data subjects rights similar to those afforded by the Directive?
- Regarding Article 4(2), it should be possible for a non-EU data controller to notify in only a single Member State, rather than notifying in every Member State where processing occurs.

C. Sensitive data (Article 8)

Member State law differs substantially regarding the use of sensitive data. For instance, in Portugal, data concerning the “private life” of an individual is defined as sensitive data, so that express consent (*i.e.*, in writing) is needed to collect data on habits of consumers or on households. Similarly, in France data concerning the newspapers that a person reads is considered sensitive data, since it may disclose political opinions. Both these examples go far beyond the definition of “sensitive data” contained in Article 8 of the Directive.

In some instances, there is no need to treat sensitive data any differently from regular personal data. Under this approach, the processing of sensitive data would be illegal when this processing is not legitimate according to the data subject’s expectations or the service to be provided and when the special interests of the data subject arising out of such data are not explicitly taken into account by the data controller. It would also be possible to exempt data from the definition which is only incidentally “sensitive”; for instance, information about a data subject’s dietary preferences may potentially indicate their religion, but this should not be sufficient to cause the data to be considered “sensitive” if it is collected in the course of asking the participants in a conference what they would like for lunch. We also suggest reaching an EU-wide agreement on a commonly-accepted list of sensitive data; this would avoid discrepancies between Member States which create significant barriers and complexity for transfer and processing.

Therefore, the current Article 8 containing a prohibition against processing sensitive data and exceptions to this prohibition is too restrictive. For instance, Article 8 could be redrafted as follows:

Article 8

(a) Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life are considered special data in which a data subject has a special interest regarding the protection of his fundamental rights and freedoms.

(b) The data controller who plans to process special data under the basis of Article 7 (e) or (f) can only do so when after having explicitly taken into account the special interests of the data subject as mentioned in section (a) of this article.

(c) The data controller is required to explicitly inform the data subject about the processing of special data.

(d) Where the consent of the data subject is required, such consent must be given explicitly.

(e) Section (b) and (c) of this article does not apply to data processors who act ... [insert exceptions from current Article 8].

D. Informational rights of data subjects (Articles 10-11)

Differences in national legislation prevent firms from using single privacy notices in their relations with consumers. For example in Italy, notices must refer to the national data protection law and the Data Protection Commissioner. As a consequence, any document concerning personal data and developed globally must be rephrased locally to comply with the national law. We would prefer to see a single, straightforward notice that companies could use on promotions and in customer relations interactions in the Member States, which will give consumers information in a format that is meaningful and actionable. Requirements necessitating long notices or lengthy privacy statements may not be read and will consequently not protect the privacy interests of consumers.

E. Notification requirements (Articles 18-19)

The Directive allows Member States to specify the details of notification of data processing, which has led to a great divergence of approaches. There is a need to have a harmonised approach within the Member States on these issues.

Furthermore, notification requires a great deal of time-consuming administrative work, which offers no real added value for data subjects, since the processing of personal data has to be lawful anyway. Moreover, notifying data processing across the EU can be quite expensive both for companies and for data protection authorities, which have to develop large databases of notifications with no clear purpose.

There are several possible solutions to the problems caused by the current legal regime on notification and ways to diminish the administrative burdens on data controllers:

- Remove all notification requirements completely, because data processing must be compliant with existing law anyway.
- It should be possible to opt out of notification based on the voluntary possibility of checking the legal correctness of data processing with data protection authorities, or on the voluntary possibility to appoint an internal data protection officer (as in Germany). Thus, the mandatory obligation to notify the data protection authorities should be transformed into a voluntary scheme whereby organisations can, if they wish, submit the planned processing for evaluation. Opting out of notification should also be possible if a company has affiliates in more than one Member State and has appointed a data protection officer. It should be left to the discretion of the company to organize internally the tasks of the data protection officer that are fulfilled locally.
- This could be combined with a system requiring mandatory notification for certain sectors that are particularly sensitive (insurance, hospitals, etc.) and high-risk privacy issues.

- For those cases where notification is mandatory and where a company does decide to notify, a model form and a process of notification that could be applied in all Member States could be agreed upon. This would avoid differences in the levels of requirements and avoid unsuitable administrative formalities. The Directive should include a mandatory simplified regime of notification and not leave this to the Member States.
- It should be possible to file one single notification in one Member State and automatically benefit from mutual recognition in other Member States. Alternatively, a single EU centralised notification process, which would be valid in all Member States, could be established. Data controllers should be able to submit the notifications in one language only with the possibility for a concerned data subject to request a translation in his/her own language.

F. International Data Transfers (Articles 25-26)

All of the existing legal bases for transferring personal data from EU Member States to third countries have significant disadvantages, particularly for companies doing business on a worldwide scale. For instance, the transfer of personal data based on consent of the data subject is quite restricted in many instances (such as in the case of transferring employee data, since many data protection authorities are of the opinion that employees cannot meaningfully consent to the processing of such data because of their inherent dependency on their employers); adequacy decisions (such as safe harbour) are limited to a small number of countries; use of data transfer agreements requires authorisation of data protection authorities from most Member States from which data is to be exported; the Commission's approved model clauses are unrealistically burdensome and divorced from business realities; and approval of codes of conduct for data transfer on a sectoral basis involves lengthy discussions with the Article 29 Working Party. It is imperative that a truly global solution for data transfer be developed which avoids the problems inherent in the existing legal bases. The following are some suggestions:

- It should be possible to transfer data when the transfer is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection (analogous to the grounds for data processing under Article 7(f) of the Directive).
- Companies should be able to transfer data based on company-wide codes of conduct that are preferably either approved by the Commission, or that are approved under the law of a Member State and then receive mutual recognition throughout the Community. This transfer should be lawful within all the organisations of the same group, independently of the location of such companies, *i.e.*, independently of whether one of the affiliates of the group is established in a non-adequate country. A

code of conduct could thus serve as the basis for international data transfers among a group of companies.

- Exceptions to data transfer restrictions should be clarified in order to allow their increased use; an example is Article 26(1)(b), which allows for transfer when this is necessary for the performance of a contract between the data subject and the controller. Member States differ on their interpretation of this provision, and a single, liberal interpretation is needed throughout the Community so that, for example, transfers of employees' data to third countries where multinational companies have their headquarters can be facilitated.
- There is too much divergence between Member States in the implementation of adequacy decisions. For instance, Member States differ in their implementation of the Commission's decision on the safe harbor, which creates barriers to its use. Furthermore, some Member States have maintained long and cumbersome procedures to transfer data to countries deemed adequate. The procedures for transfers to companies adhering to an adequacy decision such as safe harbor should be simplified, and such transfers should be automatically authorised by the local data protection authorities.
- The Commission's model contracts are too complex and cumbersome. We would like the Commission to review them in light of the practical experiences that companies have gained through using them. In addition, the Commission should approve the alternative model contracts for controller-to-controller transfers which have been developed by the ICC, the CBI, UNICE, Amcham and other business organisations, thus giving data controllers an alternative. Companies should also have the possibility to have their own contractual clauses recognized by the Commission.
- Even the application of the model contracts is not handled in a harmonised way by Member State authorities. A number of Member States (such as The Netherlands) still require the granting of a license for data transfer even when the Commission's approved model contracts are used; while this purports to be a mere formality, it creates unnecessary burdens for data exporters.
- As a related matter, there is an urgent need for a more realistic and flexible legal regime covering onward transfers of personal data. Many data protection authorities seem to believe that personal data is transferred from the EU only once and is then locked away somewhere; in fact, in today's networked economy, data is routinely transferred on numerous occasions, which produces the need for a workable regime for onward transfers. The term "onward transfers" is defined neither in the Directive nor in most Member State implementations of it, and many data protection authorities take the position that personal data may not be transferred further by the data importer; indeed, many would not even allow onward transfers when one of the grounds for transfer under Article 26(1) is present. The uncertainty surrounding

onward transfers is causing significant problems for European companies, and it is imperative that the Commission foster a uniform legal regime for onward transfers that allows their use and the application of Article 26(1) to them.

G. Employee Issues

There is an urgent need for harmonized rules throughout the Member States on issues such as employee consent and the monitoring of employee e-mail and Internet usage. The recent study published by the Article 29 Working Party, and the study prepared by DG Employment, demonstrate how divergent Member State law is on this point, which hinders development of the internal market by preventing companies from adopting Community-wide policies in these areas.

Another issue relates to the processing of employee data in the course of “due diligence” proceedings (i.e., an investigation of a company by the buyer with the consent of the seller in the course of a merger or acquisition). In practice, it can be difficult to find a legal ground for processing personal data in the course of due diligence proceedings, which can create significant problems in mergers and acquisitions. Member State law should provide clear exceptions to the processing of data in the course of due diligence proceedings, since they present little danger to personal data and are necessary to ensure that purchasers receive reliable information about the entity they are purchasing.

H. Article 29 Working Party and Article 31 Committee

Despite the increasing importance of the papers and opinions issued by the Article 29 Working Party, the procedures under which the Working Party operates are not transparent and there is little opportunity for the public to provide input on important issues; the same is true of the Article 31 Committee. Both the Working Party and the Committee should routinely publish their meeting schedules, agendas, and minutes on the Internet, and should allow observers to participate in their deliberations (as is the case with most international organisations such as UNCITRAL, the OECD, the Council of Europe, etc.). Moreover, both bodies should engage in public consultations and solicit input from the public before they issue papers or make decisions.

For questions on this paper please contact the EPOF secretariat:

<p>Rosa Barcelo Morrison & Foerster LLP Avenue Molière, 262 B-1180 Brussels, Belgium Tel. +32-2-347 0400 rbarcelo@mof.com</p>	<p>Christopher Kuner Hunton & Williams Avenue Louise, 326 B-1050 Brussels, Belgium Tel. +32-2-643 5800 ckuner@hunton.com</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------