Analysis and impact study

on the implementation of Directive EC 95/46 in Member States

Introduction

Directive 95/46 EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was adopted on 24 October 1995 and was to be implemented by the Member States by 25 October 1998. Article 33 of the Directive says that the Commission shall issue a first report to the Council and the European Parliament on the implementation of the Directive no later than three years after this entry into force, attaching, if necessary, suitable proposals for amendments.

This article further stipulates that the Commission shall examine, in particular, the application of the Directive to the data processing of sound and image data relating to natural persons, taking account of developments in information technology and in the light of the state of progress in the information society.

At the Internal Market Council of 26 November 2001, Commissioner Bolkestein announced that the first report on the implementation of the Directive would be delayed, because the Member States were slow to transpose the Directive in national law. Indeed it has still not been transposed by all Member States.

The Commission decided in December 1999 to take France, Germany, Ireland, Luxembourg and the Netherlands to the European Court of Justice for failure to notify all the necessary measures to implement Directive 95/46. In 2001 the Netherlands and Germany notified and the Commission closed the cases against them. France notified the data protection law of 1978 so that the proceedings against that state were dropped. France announced at the same time its intention to pass a new law that is not yet adopted. In the case of Luxembourg, the Commission action has led to this Member State being condemned by the Court of Justice for failure to fulfil its obligations. The Directive was then implemented with a new law that entered into force on December 1, 2002. In the case of Ireland, the infringement procedure still follows its course. The *European Communities (Data Protection) Regulations, 2001* were signed by the Irish Minister for Justice, Equality & Law Reform on 19 December 2001, and brought into force Articles 4, 17, 25 and 26 of the Directive with effect from 1 April 2002. A complete bill was recently passed but not yet notified to the Commission.

This Directive serves the double purpose of ensuring the free movement of personal data in the Internal Market on the one hand, and guaranteeing a high level of protection for data subjects, on the other. It generally sets out a high level of normative density with the result that Member States cannot go beyond nor fall short of these standards. There are, however, specified areas where Member States have, under certain conditions, a margin of manoeuvre in their implementation.

Further to that, it is important to bear in mind the broader legal and political framework, in particular the principles of Convention 108 of the Council of Europe. Both the Convention and the Directive enshrine a fundamental right recognised since 1950 by the European Convention of Human Rights and since the year 2000 recognised by Article 8 of the Charter of Fundamental Rights of the European Union.

The analysis is in part based on two independent studies commissioned in 2001 and 2003. In order to additionally collect as much information as possible as regards the practical functioning of the Directive, the Commission sent questionnaires to Member States and national data protection authorities. It published a call for comments and received 73 position papers in response, mostly from industry and business associations. Further to that, the Commission launched an online consultation for data controllers and data subjects to which it received more than 12 000 replies. Although not considered to be scientific or representative, the replies served as an additional source of information for this analysis. Finally, it held an international conference with more than 400 participants[1].

This analysis concentrates on, but does not exclusively deal with, the Internal Market aspect of the Directive. It is important to underline that the assessment is not meant to be exhaustive, but rather gives examples of provisions in the transposition laws and the most important divergences detected. The Commission has made every endeavour possible to ensure that the content of the report is accurate but should there be any omissions or inaccuracies it accepts responsibility for such errors.

Given the relatively little experience that exists with the application of the Directive in practice, the analysis tends to concentrate on aspects that have clearly emerged already. Some articles, as for instance Articles 29-31, do not require transposition and are therefore not dealt with.

[1] For further information please consult our homepage at www.europa.eu.int/comm/privacy

Part one: Analysis of transposition legislation

1. Definitions (Article 2 of the Directive)

In spite of considerable general convergence, the definitions in the laws of the Member States still differ in detail.

As regards the concept of 'personal data' most Member States follow the definition in the Directive quite closely, with some of these, however, not including the detailed clarification provided for in the Directive as to what is to be regarded as an 'identifiable' person. The French data protection law of 1978 mentions that the concept of 'nominal information', as the law terms it, covers data 'in whatever form' that allow, directly or indirectly, the identification of a natural person. The UK law makes a formal distinction between 'data' and 'information'. The Finnish law uses a wide definition of personal data that cover 'any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household'.

There appears to be division among Member States on whether or not to use a relative approach to the concept of personal data in the sense that data are considered personal only for someone who can link the data to an identified individual. The laws in some Member States make clear that for instance encoded or pseudonymised data are 'personal' with regard to a person who has access to both the data and the 'key', but are not personal with regard to a person without access to the 'key'. The Austrian law refers to such data as 'indirectly identifiable data', while other laws add definitions of pseudonymised data, like for example the German law. The UK law considers only '*data relating to a living individual who can be identified 'from those data or… from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller '* as personal data.

In other Member States, like for instance in Belgium, in principle all data, which still *can* be linked to an individual, are regarded as 'personal' even if the data are processed by someone who cannot make that link. The laws in several other Member States are ambiguous in this respect, with the data protection authorities of these Member States tending to agree with the Belgian approach, but they are willing to be flexible with regard to the processing of non-immediately identifiable data . In the case of such processing the question of whether the laws apply is related to the probability of the data subject being identified, with the nature of the data also taken into account. From this it follows that diverging use is made of recital 26 of the Directive, with some emphasizing the term 'likely reasonably to be used', and others rather relying on the expression 'to be used either by the controller *or by any other person*'.

The laws in most countries apply to 'natural' or 'physical' persons, and consequently do not apply to deceased persons. Some laws make this explicitly clear by referring to 'natural living persons' or 'living individuals'. Some laws apply to deceased persons, for instance the Portuguese law in an interpretation by the national supervisory authority on the basis of a joint consideration of the data protection law and provisions of the

Portuguese civil code, and others contain special provisions or are interpreted in this way by the data protection authority, eg allowing close relatives of a deceased patient access to the latter's medical file (Luxembourg), allowing these provisions to require controllers who have not yet recorded that fact to rectify this omission (France).

The laws in Austria, Italy and Luxembourg extend the concept of data subject to legal persons.

The laws of most Member States contain definitions of the term 'processing' that are at least similar to the one set out in the Directive, but with a significant amount of variation, omission or addition. For example, the law in Germany limits the concept of disclosure to transmissions to a third party.

As regards the 'personal data filing system', differences appear to be more obvious. Several Member States do not add the clarification provided by the Directive as concerns decentralised or dispersed systems. Whereas the Finnish law defines the term somewhat differently to the Directive as a set of personal data composed of markings belonging together due to their purpose of use and processed fully or partially automatically, or sorted into a card index, directory or other manually accessible form so that the data pertaining to a given person can be retrieved without unreasonable cost', the UK uses an apparently narrow definition that refers to a set of data which is 'structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible'. The German law defines 'automated processing' separately from the concept of 'non-automated data sets' and defines the latter, differently to the Directive, as any collection of personal data which is 'organised in similarly structured [parts]' and which can be 'accessed and evaluated according to specific criteria'.

Some textual divergences can be found in the definitions of the term 'controller'. Thus, some countries define it as the person who determines 'purposes and manner' (Italy, UK) or the 'purposes, contents and use' (Spain) or the 'scope and manner' (Greece) or the 'purposes' only (Austria) of the processing; another defines the controller as the person/s , corporation, institution or foundation, or a number of them for whom the filing system is established and 'who is entitled to determine the use of the file' (Finland), and yet another sees it as the entity that 'collects, [further] processes or uses personal data for itself' (Germany). Many national laws have included the phrase 'alone or jointly with others' for which the Directive itself provides. Most laws define the term 'processor' in the same terms as is done in the Directive, with the Spanish law adding 'alone or jointly with others' to this definition. The laws in Finland and Germany do not define the concept specifically, but refer to the concept of somebody processing on behalf of the controller or on instructions set out in other definitions. The same applies to several Member States' laws as regards the concept of 'third party', whereas others follow the definition in the Directive. As regards the definition of 'recipient', several Member States follow the Directive closely with the notable exception of the exclusion of 'authorities which may receive data in the framework of a particular inquiry' in the laws of several Member States (Greece, the Netherlands, Germany), and which the Belgian and Swedish laws limit further. The UK law specifies that a recipient can be a data processor or an employee or agent of a data controller or processor. There is no explicit definition of all these terms in the French law.

Several Member States define the data subject's 'consent' in accordance with the Directive, albeit sometimes with additions such as 'unambiguous' (Sweden, Spain),

'explicit and unambiguous' (Luxembourg), details about the information that has to be provided (Greece) or the requirement that consent has to be given in writing (Italy and Germany, in principle). As regards the element that a valid consent must include a clear indication of the data subject's wishes, most data protection authorities have taken the view that such is for instance not the case when the possibility to opt-out is foreseen and the data subject does not reply, because such silence does not clearly indicate the wishes.

Neither the French nor the UK and Irish laws define the concept of 'consent' at all. It appears that under UK and also Finnish law in some cases implied consent may be valid but not if the data is sensitive data, so the character of the data gathered is significant in this regard.

Almost all laws contain definitions in addition to the ones foreseen in the Directive. Often these are merely short references, further definitions of terms such as 'sensitive data' or 'third country' or definitions of concepts specific to that Member State, such as e.g. personal credit data in the Finnish law or 'sources accessible to the public' in the Spanish one. Some concepts, however, stand out as additions. Thus the laws in Portugal, Greece, Luxembourg and Austria add definitions of 'interconnections', 'combinations of data'and 'linked data files' respectively. Several laws also include definitions of data blocking as well as 'anonymising' and 'pseudonymising', as already mentioned above.

2. The substantive scope of the national laws (Article 3)

The Directive requires the Member States to apply its provisions to all automated processing of personal data and all processing of such data involving 'structured' manual files, if processing takes place within the scope of Community law and is not carried out for purely personal or household activities. Most Member States apply their laws to processing by means of both automated and 'structured' manual systems. However, some countries extend the rules to (some) manual processing not involving such a system. The scope of the laws is also affected by the differences in the definitions mentioned above. As a result, some divergences remain in spite of a large measure of convergence on paper.

As already noted above, three Member States, Austria, Italy and Luxembourg extend protection quite generally to legal persons, and Denmark to certain data on such persons, while in Germany some limited protection under more general legal concepts could possibly be granted.

The laws in all Member States apply, in principle, to matters both within and outside of the scope of Community law, even though they also often contain specific exemptions concerning typical 'third pillar' issues such as police or state security matters, as regards the information provided to the data subject. Thus, Member States have generally not availed themselves of the possibility to limit the scope of the national laws to matters within the scope of Community law.

Member States have also made rather limited use of the possibility to fully exclude from these laws processing related to the matters listed in Art. 3 (2), first indent, of the Directive. The Irish, and Spanish laws have such full exceptions for areas such as police, security and/or terrorism and serious organised crime. Other Member States subject some or most processing in the areas listed in Art. 3 (2), first indent, to separate laws, but this does not necessarily mean that they are subject to a regime which is not supposed to

be compatible with the principle of the Directive. Such laws in the Netherlands, Germany, Italy and Luxembourg touch on police, security and sometimes defence matters.

Finally, the status of national laws implementing the Directive within the domestic framework of laws differs considerably. In some Member States the law in question is regarded as quasi-constitutional, or otherwise overriding other legal provisions, while in others the Parliament can pass laws which amend or alter the effect of the laws implementing the directive. This seems to be the case, at least, in the United Kingdom and Sweden.

3. The national law applicable (Article 4)

In order to determine the territorial scope of the national laws with a view to avoiding both conflicts of law as well as lacunae where no law applies- the Directive requires Member States firstly to determine the controller's establishment as grounds for an application of the respective Member State's law as a principle (the provision with regard to the Internal Market) and, secondly, if the controller is not established on Community territory, to apply their law if the Controller makes use of equipment situated on their territory (the provision applying to Controllers in third countries only).

As regards the first main rule, several Member States use the same wording as the Directive. Others follow the Directive closely and add that the laws apply to a controller 'in respect of any data' (UK) or 'in respect of the processing of personal data' (Ireland).

The Finnish, Swedish and Greek laws all refer to processing of personal data where the controller is situated or established on the territory of that Member State, i.e. none of them refer to the processing having to take place "in the context of the activities of" the establishment of the controller in question. None of the laws explicitly specify that they do not apply to processing on their territory if the processing takes place in the context of the activities of an establishment of a controller in another Member State, or to processing by a controller who has its main office on their territory but when the processing takes place in the context of an establishment of that controller in another Member State. However, the non-applicability of domestic law is expressly mentioned in the Explanatory Memoranda to the Dutch and Belgian laws and also appears to be implicitly accepted by the other countries just mentioned. The Luxembourg law says it applies to 'processing carried out by a controller who is subject to Luxembourg law'. This must presumably be read as covering both controllers established on Luxembourg territory and those who are not established there but subject to Luxembourg law by virtue of public international law. The ambiguity in this crucial context is, however, not helpful.

The Austrian law stipulates that its provisions apply to "processing of personal data in Austria", except that if a controller who is established in another EU Member State processes personal data in Austria, the law of the place of establishment of that controller is to be applied, unless the processing is for a purpose which "can be attributed to an establishment of the controller in Austria". To this, the law adds that "legal provisions departing from the above rule" are "permissible only in matters outside the scope of Community law". The latter is recognition of the fact that the main rule in Art. 4(1) of the Directive only applies to matters within the scope of Community law. While it still retains that rule, in principle, for matters outside the scope of Community law, it

allows for corrective measures if the application of this rule leads to data subjects being deprived of adequate data protection in particularly sensitive matters, such as those relating to the "third pillar".

By contrast, the laws in Denmark, Germany, Italy and Spain contain provisions on their territorial application that in some respect differ from the general rule set out in the Directive.

Thus, the Danish law applies to "processing of data carried out on behalf of a controller who is established in Denmark, if the activities are carried out within the territory of the European Community." The latter qualification means that the Danish law does not apply to processing by a controller established in Denmark, with regard to activities in third countries which have no connection with activities in the Community. The qualification is apparently based on the Danish version of the Directive - but if that is the case, it would appear that that version is not in line with the other language versions, which do not contain such a limitation. In recognition of the fact that adequate data protection is not ensured by the Directive with regard to matters outside its scope, the Danish law furthermore stipulates that it does apply to processing in Denmark by a controller established in another EU/EEA Member State, if the processing is not subject to the Directive, i.e. if the processing relates to matters outside the scope of Community law. It follows, *a contrario* and in line with the Directive, that the law does not apply to processing in Denmark by a controller established in another EU\EEA Member State if the processing is subject to the Directive.

The German law distinguishes between processing in Germany by a controller established (*belegen)* in another EU\EEA State, without this involving an establishment (*Niederlassung)* of the controller in Germany, and processing in Germany by a controller established in another EU\EEA State but which is carried out by an establishment of the controller in Germany. The law does not apply in the first situation, but does apply in the second situation. However, the law does not clarify to what extent it itself applies extraterritorially. The Italian law applies to "processing of personal data, by anyone, carried out on the territory of [Italy]"; and the Spanish law to "processing [which] is carried out on Spanish territory as part of the activities of an establishment of the controller." Neither of these rules appear to properly reflect the first main rule in Art. 4(1)(a) of the Directive. The French law uses the criterion of location of operations of data processing on the territory of France.

The above differences in the implementation of the first main rule in Art. 4 of the Directive result in the very kinds of conflicts that Art. 4 of the Directive seeks to avoid. Clearly, this is partly the result of deficient transposition of the Art. 4 of the Directive; a deficient transposition which could be partly explained by the complexity of that provision itself.

As to the second main rule in Article 4, whereby Member States must in principle apply their laws if the controller is not established on Community territory but makes use of equipment situated on the territory of that Member State, again, several Member States avail themselves of the wording used in the Directive. Other laws use some variations and extensions.

First, many laws use a term which translates into English rather as "means" than "equipment" (F: moyens, I: mezzi, P: meios, E: medios, DK: hjaelpemidler), which

appears to be wider than "equipment", which suggests a physical apparatus. In fact, all processing appears to involve "means". The German[2] and Austrian laws indeed apply to processing in these countries respectively, without the law using the term "means".[3] As regards the provision in the Directive by which controllers have to designate a representative in case they make use of such equipment, the Greek law extends this requirement beyond the situation envisaged in the Directive when it requires all controllers outside Greece to appoint a representative if they process data on Greek residents. Secondly, there is some confusion over the exception for controllers who use equipment for "transit through the territory of the Community", as the Directive states. Several laws refer to transit through the Member State in question instead of the Community, others merely to „transit" without clarifying whether this means transit through their territory or the EU. The Swedish law applies the exception, if the equipment "is only used to transfer information between a third country and another such country". The French law does not contain this second rule of Article 4.

In conclusion, it must be noted that there is no complete uniformity yet in the implementation of the 'applicable law' provision. Because of the substantial divergences, potential positive and negative conflicts of law remain between the Member States.

4. Data Quality (Article 6)

The Directive lays down a number of principles that contain the fundamental requirements to be met by any processing of personal data.

These data protection principles of Article 6 are set out in very similar or slightly varying terms in the laws of most of the Member States. There are more substantial differences between the Directive and the French law that only prohibits any collection of data in an unfair or unlawful way, and foresees that nominal information may not be kept in a form which permits identification for no longer than necessary for the purposes for which the data where collected or processed. The law does not contain however any further principles. The German law also does not contain a list of principles but refers to most of them throughout the law. It also adds some more principles, i.e. that data should be collected from the data subject. In addition, some Member States add clarification to the principles in ways which sometimes strengthen them, as is the case in the Netherlands, but sometimes do the opposite. In the UK for instance, the law adds fixed interpretations to the principles. Thus, the law adds an interpretation of the first principle (that personal data must be processed fairly and lawfully), to the effect that personal data are always to be treated as having been obtained fairly if they were received from a person who was "authorised by or under any enactment [law] to supply it", provided that the rules relating to the provision of information to the data subjects are complied with.

---

[2] In its response to the questionnaire of the Commission on the implementation of the Directive the German DPA held that if referring to the "means of the Internet" it would be decisive in order to dtermine the applicable law who has factual control of the hardware.

[3] The Belgian Commission in its response to the questionnaire held that there may be difficulties in interpreting "means located on Belgian territory".

For the purpose of this analysis, it might suffice to examine by way of example how the crucial principles of purpose specification and –limitation and incompatibility of purpose have been implemented in the Member States, and how their laws regulate the further processing for research purposes.

The purpose-specification and –limitation (Zweckbindungs-) principle is set out in terms identical or very similar to the ones used in the Directive in the laws of most of the Member States. There is a considerable amount of case law within the data protection authorities on the subject, and several authorities have issued detailed guidance. However, in spite of the similar wording, the flexibility of the principle leaves it open to divergent application, and different Member States apply different tests in this regard. As concerns the notion of "specified purpose", the UK law for instance, and uniquely, stipulates that the purpose of processing may be specified "in particular" in the information given to the data subject or in the particulars notified to the data protection authority.

The same divergent application seems to take place as regards the "incompatible use" criterion. Member States' laws range from the "reasonable expectations" of the data subject (eg in certain cases Belgium), to "fairness" (e.g. Greece*: 'lawful processing if data are collected fairly and lawfully for specific, explicit and legitimate purposes and fairly and lawfully processed in view of such purposes'*) or the application of various "balance" tests (e.g. Germany without express reference to the principle, and the Netherlands, on the contrary, adding a list of criteria that would help to strike that balance) to determine incompatibility. In France, the criterion does not appear as such in the law, however, the French data protection authority, the CNIL, points out that the application of Convention 108 of the Council of Europe guarantees the respect of this principle that, in addition, is checked by the CNIL at the time of the notification of a processing. According to the doctrine of the CNIL, the control of compatibility is all the more rigorous if the processing takes on an obligatory character or if the data are covered by legally protected secrecy.

The rules concerning secondary processing of personal data for research purposes, contained in the laws of the Member States, vary very considerably. Some fail to provide any safeguards, some lay down minimal safeguards, e.g. that the data may not be used to take decisions on the data subjects, or may only be used for the research in question ; and some lay down rather abstract "balance" tests or only say that the research must be based on an "appropriate research plan". On the other hand, the laws in some countries provide for detailed rules which limit the data and the processing and stipulate that the research must be approved by an "ethics committee", or require researchers to apply for a special authorisation from the data protection authority (Belgium), who is to stipulate various conditions, or these additional conditions may be spelled out in the law already (Greece, Luxembourg and Portugal).

It appears that by reason of their open-ended nature, the principles are clearly capable of being differently applied in different Member States, and indeed likely to be differently applied, even in comparable cases, since some countries take a very strict view of them while others adopt a more relaxed approach. Also, they are applied in a very casuistic manner, and the cases in which individual Member States have provided clarification differ between them.

5. Criteria for making data processing lawful (Article 7) and processing of special categories of data (Article 8)

To the list of principles contained in Article 6, the Directive, in Article 7 adds a further list of criteria. These determine the lawfulness of any processing and in this way establish the link back to Article 6 that provides that personal data must be processed 'lawfully'.

As regards the implementation of the criteria for making processing legitimate, several Member States set out these criteria basically as in the Directive. In others, the laws take a more hierarchical view in that the criteria 'consent' and 'processing based on a law or to fulfil a legal obligation' are given primary status with the other criteria seen as exceptions to these primary criteria. These criteria are as such not part of the French law.

It would go too far for the purposes of this analysis to examine the implementation of all criteria in each Member State. Instead, we shall see how Member States implemented the "consent", "processing in the public interest/in the exercise of official authority", and "balancing of interests" criteria contained in Art. 7 (a),(e) and (f). The laws in the Member States all allow for the processing of personal data on the basis of consent, in terms identical or close to those used in the Directive, albeit with some differences in emphasis and with some adding additional clarification or requirements, e.g. that consent must in principle be given in writing, such as the German legislation stipulates or be documented in writing ('documentata per iscritto'), as the Italian law terms.

Most of the laws examined allow for processing which is "necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed" (Art. 7 (e)) in precisely these terms, without additional clarification. The laws in other Member States are in principle more restrictive, in that they require that the task or function concerned must be specified by law.

However, these constraints are undermined in several of the Member States by more general, and more relaxed, rules which allow for processing whenever this is "authorised by law" or by "special provisions" in or even adopted under any law. Such other laws or provisions will often relate to exactly the kinds of tasks or functions envisaged in the above-mentioned criterion - yet in some Member States, there is no guarantee that processing on the basis of such other laws or rules will be limited to what is "necessary" for the tasks or functions in question.

The public sector in all Member States is governed by particular principles, such as the legality principle, the basic rule being the possibility to process data if necessary for the performance of a task carried out in the public interest .

The "balance" criterion, Art. 7 (f), is set out in the words used in the Directive or in very similar terms in the laws of only eight Member States. Several of these intend to issue further clarification on its application but have not yet done so - but the kinds of matters to be taken into account are clear from other Member States: the nature of the data; the nature of the processing; whether the processing is carried out in the private sector or the public sector (with the latter being subject to a stricter assessment); and the measures which the controller has taken to protect the interests of the data subject. In one country, Germany, somewhat differently phrased tests are applied to the private sector and the public sector, respectively. By contrast, the test is applied more restrictively than in the Directive, and/or subject to further formal requirements, in the remaining countries.

These either "tilt the balance" decisively towards the data subject, or limit its application to certain narrowly defined data, or to cases specified by the Data Protection Authority. In one country, Finland, the law sets out a limited number of cases in which data can be processed and which can be seen as special applications of the "balance" test, but otherwise requires controllers who believe they can rely on this test to obtain a permit from the Data Protection Authority.

The situation in Spain in this regard is also peculiar. The absence of this provision in the Spanish Data Protection Law is justified by the government, in the sense that the legislator, similarly to the Finnish one, sets out those cases where the balance test authorises controllers to carry out the processing of personal data. Consequently, in Spain, such processing operations would be those necessary for credit reporting purposes, insurance purposes (e.g. aimed at identifying fraud) and any operations involving the processing of certain type of data which would be made publicly available from the so-called publicly available sources such as the promotional census, the telephone directories, official journals, etc. This peculiarity together with the fact that the Spanish law confers a special treatment to processing that consists of disclosure of information to a third party ("cesion de datos") makes the processing of personal data without consent of individuals considerably more difficult in Spain than in other countries.

Overall, there is therefore again quite substantial divergence between the Member States.

Generally speaking the specific dangers for the protection of fundamental rights and freedoms are determined not only by the content of the data but also by the context in which they are processed. There exist, however certain categories of data which, because of their content, involve the risk of infringing such rights. Therefore Article 8 of the Directive lays down additional conditions, over and above the usual criteria for making processing lawful set down by Art.7, for the processing of these so-called "special categories of data", more commonly referred to as "sensitive data". Article 8 is a general prohibition with the possibility for exceptions. It has to be noted that these exceptions are often subject to secondary legislation, the examination of which goes beyond the scope of this analysis.

5.1 Art 8(1)- Definition of sensitive data and the in-principle prohibition

Most Member States set out categories of data to be regarded as sensitive as is done in the closed list of Article 8 (1) of the Directive. Some Member States, however, add further categories or treat certain categories specially even if they are not formally included in the concept of "sensitive data". For instance, in Finland "special categories" include data on social affiliation, social welfare benefits and socially oriented actions targeted at a data subject, e.g. taking children into custody by social welfare authorities, while the Greek law also regards membership in any association and data on social welfare as sensitive. Several countries including Denmark, Greece and Portugal impose restrictions on data on purely private matters, creditworthiness or debts, Finland imposes restrictions only on data on creditworthiness. In certain countries criminal convictions are also included under the category of sensitive data although the Directive covers such data under Art. 8(5). The Netherlands' definition also includes personal data connected with "unlawful or objectionable conduct for which a ban has been imposed". The French

law neither considers ethnic origin nor data concerning health or sex life as sensitive data, but refers to 'moeurs des personnes'[4].

As regards the implementation of the term 'revealing' the personal attributes, several Member States' laws repeat this wording, whereas others use terms such as 'referring to' 'relating to','as to' or 'on' or "describe or are intended to describe". These different terms may have implications in particular as concerns matters which can be said to indirectly 'reveal' sensitive matters.

5.2 Art. 8(2)- The exceptions to Art. 8(1)'s prohibition

Art. 8(2) sets down the exceptions to Art.8(1)'s prohibition. All the Member States follow this approach but with some variation or additions.

Some Member States set down additional requirements like prior opinions and prior authorisations for the processing of sensitive data, even if it falls within one of the exempted/permitted categories. Spanish Law requires written or legal authorisation for the processing of certain sensitive data (those revealing ideology, religion, beliefs or trade union membership) in connection with the special protection provided for these data at constitutional level. For all other sensitive data, the Spanish law follows the rule set out in the Directive, that is, that consent must be explicit. In Portugal, processing of sensitive data on "important public interest grounds" and even processing with the explicit consent of the data subject requires the authorisation of the data protection authority.

This analysis only deals with the exceptions foreseen by Article 8 (2) (a) and (b). As regards the exception in case of the data subject's explicit consent in Article 8 (2)(a), several laws use the same term as foreseen in the Directive. Many data protection authorities have issued guidance on the subject, or are planning to do so. The Dutch data protection authority, for instance, considers a consent explicit if 'the data subject has expressed itself actively as to the scope of the consent'. In France, case law interpreted the requirement in the law of "express consent" for the processing of sensitive data as requiring that the consent be expressed *in writing* - although the data protection authority has accepted that, with regard to processing of sensitive data on the Internet, one may substitute a "double-click" for this consent, i.e. one "click" to confirm that one is aware of the proposed processing, and a further one to "expressly" consent to it. According to the Portuguese data protection authority, express consent for health data means written consent. Th Italian law stipulates that consent must be given in writing and in addition to that requires a prior authorisation by the data protection authority.

In Belgium a decree provides that consent of an employee may not be used to allow processing of sensitive data, including medical data, by a present or future employer. This prohibition of processing is extended to circumstances where the data subject is in a *'relation de dépendence'*. Under the Finnish Act on data protection at the workplace of 2001, the employer is only allowed to process personal data that is directly necessary for the employment relationship and concerns management of the rights and obligations of the parties to the relationship or benefits provided by the employer for the employee, or arises from the special nature of the work concerned. No exceptions can be made to this provision even with the employee's consent.

---

[4] A notion that might best be translated meaning 'manners, morals, customs or habits'.

With respect to the exception for processing of personal data under employment law one group of Member States has worded provisions that add very little or no detail to the provision of Article 8 (2)(b). In others, the matter is left to special domestic laws which apply in this field such as equal opportunities/anti-discrimination legislation, ethnic composition requirements or legislation on criminal records which addresses the issuing of certificates of good behaviour by relevant local authorities. The first national legislation in the EU dealing specifically with data protection at the workplace is the Finnish Act of May 2001 on protection of privacy in working life. This law is not restricted to regulating the processing of sensitive data in the employment context, however. The special legislation on workers' data protection envisaged by the German federal government has yet to be delivered.

An exhaustive examination of existing secondary legislation goes beyond the scope of this analysis. We therefore keep to mentioning a few examples in this important area that deserves further elaboration in the future.

According to the Finnish Act referred to above, the employer has the right to process information concerning the employees' state of health only if the information has been collected from the employee him/herself or elsewhere with the employee's written consent and is needed for reasons related to the employment, such as ie to pay sick benefits. In the UK, there are a number of rights and obligations conferred or imposed on employers by statue or common law, which may legitimise processing of sensitive data regarding workers. The second part of a code of practice that contains provisions on this issue has recently been published by the Information Commissioner, with further codes under consideration. The Data Protection Authority in Greece has issued supplementary guidelines on the protection of the personal data of workers, which is binding on its addresses. The French labour code prevents employers from collecting certain data with a view to recruiting even where this data could be obtained directly from the data subjects. The Netherlands allows employers to process personal data concerning health where this is necessary to provide benefits, which are dependent on the health of the person concerned or for the reintegration of sick or disabled employees. Also in the Netherlands, the so-called law SAMEN (Act on the Stimulation of Labour Participation by Minorities) allows the processing of a limited set of data on the ethnic origin in order to allow positive discrimination at work.

5.3 Article 8(3)- medical data

This provision allows an exemption from the application of Art.8(1)'s prohibition on processing, where the processing is necessary for the purposes of preventive medicine, medical diagnosis, provision of care, treatment or management of healthcare services. Most Member States transpose this provision into national law in similar terms while in the Netherlands also include the processing by insurance companies of such medical data where necessary for assessing risk and the data subject raises no objection.

The Netherlands also foresee exceptions for schools processing such medical data if it is necessary for providing pupils with special support or for making special arrangements in connection with their health and for administrative bodies, pension funds, employers or institutions working for them if required by law, by collective agreements or for the

reintegration of or support for workers entitled to benefit regarding sickness or work incapacity[5].

The Italian legislation allows for processing of health data without the authorisation of the Garante where it is required to safeguard the data subject's bodily integrity and health[6].

All the Member States' laws refer to the legal obligation of confidentiality or the requirement to treat data with confidentiality although not required by law.

5.4 Art. 8(4)- substantial public interest

The Directive allows the Member States to lay down further exemptions, provided that the processing is justified by reasons of substantial public interest.

Such exemptions are often subject to secondary legislation and are thus not exhaustively covered by this analysis. It should also be mentioned that provisions adopted on the basis of Article 8 (4) are only very rarely notified to the Commission by Member States[7], contrary to their obligation set out in Article 8 (6). The Commission therefore has an incomplete understanding of the implementation of Article 8 (4).

From this the Commission gathers that the laws in the Member States provide for few specific exemptions to the in-principle prohibition on the processing of sensitive data, on the lines envisaged by Article 8 (4), although several of them allow for the adoption of subsidiary rules of this kind or the issuing of ad hoc authorisations. Such authorisations have only been issued by France and the UK until now.

Since 1994 French law has specific regime on the processing of health data for the purpose of medical research under specific conditions. There are also decrees authorising the recording of civil agreements between same sex partners so as to enable the couples to avail of entitlements similar to those enjoyed by spouses and decrees regarding public security, anti-terrorism, defence and state security.

---

[5] The law in the Netherlands also has an interesting reference to personal data concerning *inherited characteristics*, which can only be processed in relation to the data subject from whom the data have been obtained, except where a serious medical interest prevails or the processing is necessary for the purpose of scientific research or statistics.

[6] Where the selfsame purposes concern a third party or the public as a whole and the data subject fails to give his consent, the data may be processed upon authorisation by the Garante. Also simplified arrangements for obtaining the data subject's consent and for such processing are provided for with regard to public health care bodies, health care bodies and professionals who have entered into an agreement with the National Health Service in Italy.

[7] The Commission has only received notifications from two Member States to this date: from the UK about the Processing of sensitive personal data order 2000 and the Data Protection (Processing of sensitive personal data)(Elected representatives) Order 2002; and Finland on the decision of the data protection board to grant authorisation to the Finnish slot machine association to process sensitive personal data.

In the UK a special Order covers ten contexts in which sensitive data may be processed. In five of these, the relevant paragraph specifically stipulates that, for the exception to apply, the processing covered must be "in the substantial public interest".

One such provision is for the purpose of research which is in the substantial public interest. This also applies in Belgium and Luxembourg regarding historical, statistical and scientific research, in Sweden with the consent of the Research Ethics Committee and in Denmark regarding legal information systems, scientific research and statistical studies. When important public interest demands it, the Data Protection Board in Finland can give permission to handle personal data even if the purposes of the processing does not fit into the exception categories stated in the Act. The Finnish Data Protection Board has used this authority to grant a dispensation to banks and insurance companies to maintain records of disruptions in customer relations.

The absence, in other Member States, of special Art. 8(4)-type exemptions, either laid down in law or issued in the form of special subsidiary rules, does not mean that no processing of this kind is allowed in these Member States. Specifically, as repeatedly mentioned, in several countries the data protection law either defers generally to "any other law" or "any legal provision", or even to administrative decisions taken under any other law or any other legal provision. This means that in the countries concerned- in particular, Germany, Portugal[8] and Sweden, and to a lesser extent Spain- processing of sensitive data can take place on the basis of such other laws or rules. In some of these, there is no formal guarantee that such processing will be subject to the "suitable safeguards" demanded by the Directive, but in some, in particular, in Sweden, the authorities are reviewing such other laws to ensure that they conform to the Directive.

5.5 Art. 8(5)- criminal convictions and offences

Again, the Commission has very rarely been notified by Member States of the derogations applied to Article 8 (5).

As mentioned above, criminal offence data is included in the Finnish, UK and Greek definition of sensitive data so this allows any of the Art 8(2) exceptions to apply including that of consent of the data subject. This potentially allows for a more relaxed approach to such data than allowed by Art. 8(5) which makes express provision for suitable safeguards. The Greek law requires also a permit issued by the DPA and it includes the safeguard that such a processing can be carried out only by a public authority. Moreover there are specific legal provisions concerning the criminal records. The Belgian law extends the restrictions on the processing to data on any legal disputes and to mere suspicions.

To mention just a few examples, the Danish legislation implementing this provision for instance states that 'private individuals and bodies may process data about criminal records, serious social problems and other purely private matters' other than those mentioned in Article 8 (1) of the Directive if the data subject has given his explicit consent. Processing may also take place where necessary for the purpose of pursuing a

[8] In the view of the Portuguese Data Protection Authority, the fact that they are requested under law to provide an opinion on every draft legal provision containing data protection matters, should be considered as an additional safeguard for such data processing being dealt with in conformity with the Directive.

legitimate interest and this interest clearly overrides the interests of the data subject. However, such processing is subject to prior checking by the supervisory authority, and the data may in principle not be disclosed without the explicit consent of the data subject. In Sweden there is provision for checks on records of staff involved in pre-school activity, school and care of school children and regarding money laundering records.

5.6 Art 8(7)- national identity numbers

Paragraph 7 contains an open-ended provision on national identification numbers. Such numbers are not used in every Member State and where they are used, there are great divergences in the rules regulating such processing. In Ireland the PPS (Personal Public Service Number) is used only for dealings with public authorities. It has been made an offence to transfer information between specified bodies other than in respect of a transaction for a relevant purpose and the Data Protection Commissioner recently issued a code of practice on the use of the number.

France too has a national identity number (NIR) set out in a national directory (RNIPP), the use of which is subject to limitations. The RNIAM is a recently devised inter-institutional directory to identify persons in the health and social sectors. The use of both numbers seems to be only allowed for clearly specified circumstances and for clearly defined purposes so as to prevent use of the number for the creation of unregulated interconnections between public sector bodies for different purposes[9].

In Belgium, there is a national identification number broadly used in the public sector, the *'numéro de régistre national'*, also called social security number for the security sector and fiscal number for taxation purposes. However, in order to make use of this number, secondary legislation is necessary on a case by case basis. There are two such numbers in Spain- the national identification document and the passport. Processing of such numbers demands a respect for privacy with an express prohibition on the inclusion of data on race, religion, beliefs, ideology or trade union affiliation.

Legislation in Luxembourg and Portugal requires that the authorities' permit be obtained before interconnections between files or combinations of data can be made. The Greek law requires such a permit in case that the files to be interconnected contain sensitive data or the processing results to the disclosure of sensitive data or if a "unique code number" is used for the interconnection.

In Denmark quite a wide exchange is allowed between public bodies. In Finland such numbers may be processed in a number of situations such as when granting credit or collecting a debt, in insurance credit, leasing and lending activities, in credit data operations, in health and other social welfare provisions and in matters relating to public service, employment and other service relationships and their associated benefits etc.

---

[9] Under fiscal legislation however, the Tax Authorities, the Public Accounts Authorities and Customs Authorities can all use the number of inscription for persons set out in the national directory for limited purposes.

In Sweden, information about personal identity numbers may, in the absence of consent, only be dealt with when this is clearly justified having regard to the purpose of the processing, the importance of a secure identification or some other noteworthy reason.

6. Data protection and freedom of expression (Article 9)

The Directive requires Member States to lay down exceptions from the provisions in the Directive that are necessary to reconcile the right to privacy with the rules governing freedom of expression.

This clearly, and as expected, is the area where least convergence can be discerned. The laws in the Member States range from stipulating the overall primacy of freedom of expression, through wide exemptions for the press, through fewer exemptions, to a system which contains elements tantamount to prior restraint on the publication of certain information by the press. Also, some laws defer expressly to press laws or self-regulatory or quasi-imposed codes of conduct and associated regulatory mechanisms, while others set out the relevant rules in the data protection law itself.

First, it should be noted that the Danish and Swedish laws explicitly state that the provisions of the laws do not apply where this would be in violation of the freedom of information and expression. To that aim, the Swedish Supreme Court held that the 'journalistic exemption' in the Directive should be read broadly, so as to encompass all cases in which the controller exercised his right to freedom of expression.

Denmark and Finland exempt from their law altogether data that have been published by the media, provided the texts and recordings are in their original form (and are covered by the pertinent provisions of specific legislation in this field in Denmark). Apart from that, under the laws in Finland and Sweden processing for purposes of journalism or artistic or literary expression is subject to selected provisions only, such as provisions on data security and supervision over adherence to that specific duty, issuing of data protection instructions by the Data Protection Ombudsman (Finland), as well as the applicable law provision. The Danish and German Federal laws[10] expressly limit the application of the law for these purposes to the provisions on data security and confidentiality and civil liability. The Austrian law stipulates that media companies, media service providers and their employees are, in their "publishing activities" only subject to the provisions on data security and secrecy and to the data protection principles and adds that 'otherwise, the provisions of the Media Law apply'.

Some laws contain a list of exemptions, such as from the provisions to inform, the exercise of data subject's rights or only indirect subject access, and to notification and prior checks (The Netherlands and Portugal) Others have limited exemptions concerning the processing of sensitive data (Italy, Luxembourg), transfers of data to countries without adequate protection, information and access and stipulate a limited notification requirement only (Luxembourg). For instance, the Italian law exempts transfers carried out exclusively for scientific research or statistics as long as they comply with codes of conduct undersigned in accordance with the law and contains a special derogation

[10] Given that the federal state only has a so-called framework competence in this area, the law stipulates that the Länder have to provide for the mentioned exceptions in their legislation.

allowing for transfers of data by journalists, provided they act in accordance with the special code of conduct for journalists, adopted under the law.

The Belgian law is even more specific in its exceptions that also partly depend on whether the data were made public by the data subject or relate to a person's public position. In this case, the provisions on sensitive data do not apply. In addition, there is no obligation to inform the data subject if this would compromise the processing made for literary, artistic or journalistic purposes.

Under the UK law, subject to certain complex substantive and procedural conditions, personal data which are processed "solely with a view to publication of any journalistic, literary or artistic material" and whose processing the data controller "reasonably believes" to be "in the public interest" are exempt from the data protection principles, and from the exercise of data subject rights to the extent that the data controller reasonably believes that complying with the particular provision of the Act is incompatible with journalistic, literary or artistic purposes. On the contrary, the Spanish law does not refer to freedom of expression at all. It contains certain provisions relaxing its rules with regard to the processing of data derived from "publicly accessible sources", which include newspapers and the other media, but these do not apply to the collecting and processing of data for the purposes of entering them in such sources in the first place[11]. Finally, the law in Greece exempts the press from the duty to inform data subjects , and even then only if the data subjects are 'public figures'. The law allows for the processing of sensitive data on 'public figures' for journalistic purposes, but only on the basis of a special permit to be issued by the Data Protection Authority. This requirement appears to amount to a prior restraint on the press.

In this context, one should however bear in mind that '(O)ne important element that emerges from the current legislative situation in the Member States is that the media, or at least the press, are bound to respect certain rules which although not part of data protection legislation in a proper sense contribute to the protection of the privacy of individuals. Such legislation and the often rich case-law on the matter confer specific forms of redress which are sometimes considered a substitute for the lack of preventive remedies under data protection law.'[12] There is also extensive jurisprudence by the European Court of Human Rights on this subject the examination of which would, however, fall outside the scope of this analysis.

As already mentioned above, several countries, namely the UK, Germany and Italy, avail themselves of codes of practice to strike a balance between data protection requirements on the one hand and freedom of expression on the other. Some countries use these to counterbalance quite wide exceptions (notably Germany) others have the press codes of practice in addition to more limited exceptions to clarify the rules in this regard (UK, Italy). In Germany, the federal law notes that processing is regulated further

---

[11] In the interpretation of the Spanish data protection authority, this choice of the legislator means that data controllers must abide by the provisions of the Spanish data protection law except if in cases of processing for artistic, literary or journalistic purposes, these provisions create conflicts with other constitutional rights (such as the freedom of expression or information). The authority is of the view that the jurisprudence of the Spanish Consitutional Court has made sufficiently clear how to strike a balance under these circumstances.

[12] Recommendation 1/ 97 of 25 February 1997 by the Working Party 29 on Data Protection Law and the Media

in codes of conduct which provide for limited access to data held by the press and for a right of correction of erroneous information. Complaints can be addressed to a recently created complaint committee equally composed of editors and journalists. There is no implementation control executed by the supervisory authorities. In Italy , the law strongly encourages the drafting of press codes of practice; the supervisory authority takes a very active role in this drafting, and can impose changes to a draft code. If a code is approved, the authority can prohibit processing that has been carried out in violation of the code. In the UK the law allows a data controller to have regard to relevant codes of practice in considering whether it is reasonable to believe that publication would be in the public interest.

7. Information to be given to the data subject (Articles 10 and 11)

Informing data subjects of various details of the processing of their data is a crucial measure to ensure transparency in data processing and the exercise of the data subjects' rights. Also, consent can only validly be given when it is 'informed'.

The Directive therefore sets out the basic information that must be provided, and in this regard distinguishes between the situation in which data are obtained directly from the data subjects, and situations in which data are obtained from other sources than the data subjects.

The laws in the Member States vary very considerably with regard to the kinds of information that must be provided, the form in which it must be provided, and the time at which it must be provided. They also differ as to the kinds of additional information that may need to be provided to ensure a fair processing. Some of them repeat the examples given in the Directive, others give somewhat different examples, and some give no examples at all.

While some Member States stay quite close to the Directive's requirements, others have diverted considerably from them. The UK Law appears to have qualified the informing-requirement by saying that the information should be provided *"or made readily available"* and also by adding that the information must only be provided *"insofar as practicable"*.

As regards the additional information to be provided insofar is necessary to guarantee fair processing, some Member States follow the examples of the Directive quite closely. Like the Directive, the law in Austria states that additional information has to be given when necessary to guarantee fair processing. To clarify when such is the case, the law provides examples of the kinds of situations, e.g. if the data subject could object and in the Netherlands this is further detailed in the Explanatory Memorandum to the Law and is evaluated on a case-by-case basis.

Contrary to this approach, the laws in other Member States are more demanding than the Directive in that they stipulate irrespective of the necessity test indicated in the Directive that some of the additional information listed in the Directive must always be provided. When dealing with information where the data have not been obtained from the data subject, the burden on the data controller is even higher with the requirement that the information should be given in writing (Italy) or at least *"explicitly, precisely and unequivocally"* (Spain). In Greece, the controller has to inform the data subject 'in an

appropriate and express manner". He/she has to inform specifically and in writing if the controller requests the data subject's assistance.

As far as the timing of the information is concerned, there are further divergences. The Dutch law determines that the data subject must be informed prior to obtaining the personal data. When data are collected directly from the individual, in roughly half of the Member States the information must be provided at the time of collection. In other Member States the legislation is silent and the laws in two Member States are ambiguous in this regard. There are also some differences when the data have not been obtained from the data subject. Most Member States basically follow the Directive, some add ambiguity given the language used, e.g. Austria stipulates that the information must be provided "in connection with" *(aus Anlass)* the data collecting and some differ from the Directive. For example, the Greek law requires that the informing be done when the data are collected without allowing for a delay if disclosure is intended, as foreseen in the Directive, while the Spanish law stipulates that the information must be provided within three months, irrespective of whether a disclosure is intended. There is an absence of the obligation to provide information in the French law where the data has not been obtained from the data subject, but the right to be informed is part of the CNIL's doctrine and has been followed in the codes of the marketing profession.

As regards the derogation foreseen in the second paragraph of Article 11, according to which no information needs to be given to the data subject where the provision of such information proves impossible or would involve a disproportionate efforts or if recording or disclosure is expressly laid down by law, the situation is unclear from the answers received from Member States on this particular point. It seems, however, that some Member States have provided for broad exemptions in this case.

From the incomplete information gathered so far it seems that all Member States apply this derogation to the processing for statistical purposes or for the purposes of historical or scientific research and apply safeguards in stipulating for instance that such data may only be used for statistical purposes or that data must be kept safe and secure. Some Member States have extended this derogation to other purposes as well, in particular by general reference to "recording or disclosure expressly laid down by law".

8. The Data Subject's Rights (Right of access, right to object, automated individual decisions)

Data subject rights are central to any data protection system as they are the primary means to assert one's "right to informational self-determination". The Directive provides for the classical rights, such as access and related rights like rectification, erasure and blocking, while adding some 'new rights', such as a general right to object and a right not to be subject to a fully automated decision based on an evaluation of one's personal aspects.

8.1 Rights guaranteed by Art. 12 (access in its various forms and rectification, erasure and blocking)

All Member States grant data subjects the right to obtain access to their data. The overall level of harmonisation in this respect is satisfactory, irrespective of some differences. In some Member States, access requests motivate a reasonable fee while in others requests are free of charge. As regards the reasonable intervals and the timing for the exercise of

this right, despite minor differences, the general rule seems to be once a year -except if there were justified reasons- with the obligation on the data controller to respond within three months of the request. Some countries provide for shorter periods, like Denmark, where the interval is six months and the controller is obliged to respond within four weeks in principle. In Greece the data subject has a right to submit a petition with the obligation to deposit a fee which should be reimbursed if his petition is deemed valid.

Several differences exist, however, such as the fact that under the laws of Greece, Spain and Sweden controllers always have to inform data subjects, on request, of the sources of the data - and not just "any available information" as to these sources-. Examples of other national peculiarities include the Greek law which adds that the controller should specifically inform the data subject of any developments in the processing since the last access request and the German law which extends this right to data held in non-structured files in those cases where the controller processes the data "professionally" for the purpose of providing the data to others. In the absence of a provision concerning the sources of data in the French law, the data subject cannot directly obtain from the controller the information referred to in that article, but has to refer to the CNIL which, within its own competences, can ask the information from the controller.

The French data protection authority has also considered that as regards the management of careers, the evaluation data concerning employees may not be communicated as long as those are of a preparatory nature that cannot be opposed by the employees concerned.

The laws in all Member States give data subjects the right to be provided with information about the logic used in processing operations, with three Member States, Greece, Italy and the Netherlands, extending this right to all kinds of automated decisions, i.e. not only those involving an evaluation of a data subject's 'personal aspects' and Portugal even extending the right to any automated processing concerning the data subject.

All the laws provide for the right of rectification or erasure and all, except the Finnish law, also expressly refer to "blocking" in this regards. The only minor differences refer to the fact that some laws put more emphasis on the action that should be taken if disputes arise, rather than on the prior matter of the rectification by the controller in response to a request for such action, but in all cases the right of rectification seems to be guaranteed.

8.2 The data subject's right to object with particular attention to direct marketing activities (Article 14)

The general right to object

The granting of a general right to object is an important expression of the individual's self-determination with regard to personal data.

This right originates in France, having been used by the CNIL for over 20 years, yet prior to the adoption of the Directive was not widely used elsewhere. Following implementation of the Directive, most of the laws in the Member States now include this provision that is, however, applied quite differently.

Four Member States apply the right strictly to the minimum required by the Directive while six Member States have extended its scope either by stipulating the right in completely general terms or to other categories of processing.

By contrast, the laws in Finland and Sweden do not provide for a general right to object- or at least not explicitly. Both laws contain a specific provision granting data subjects the right to object to the use of their data for direct marketing purposes and a range of other, related personalised marketing activities.

The right to object to direct marketing use of one's data[13]

The Directive requires Member States to grant data subjects the right to object to either the processing or the disclosure or use of their data for direct marketing purposes. As far as the choice between the two alternatives is concerned, an about equal number of Member States have opted for each. In Austria this right is mentioned under separate legislation, § 151 of the industrial code that states that the general data protection law shall apply. This provision existed prior to the new data protection legislation so there was felt no need to change it. However for a data subject, it is not the most obvious thing to search for his rights in some hidden paragraph of the industrial code.

The rules in five further countries in effect come close to the second option too, by requiring that if data are collected from the data subject, the latter must be offered the right to object.

As far as the mechanisms for ensuring compliance with this right are concerned, special services usually referred to as "Mailing Preference Services" or "Robinson Lists" have been established to this end in all the Member States except Luxembourg but are arranged and operated in different ways. They are operated by public bodies in Denmark and Greece and by industry on a self-regulatory basis in the other Member States.

8.3 Automated individual decisions (Article 15)

This provision reflects the assumption that information technology must serve mankind and should not violate "human identity" or fundamental rights and freedoms and therefore prohibits the taking of judicial, administrative and private-sector decisions on the sole basis of automated processing of data which constitute a "personality profile".

Following the implementation of the Directive, the laws in the Member States now all contain provisions on automated individual decisions, however, with some differences.

Several Member States apply the exemptions in Article 15 (2) other than where foreseen by the Directive. For instance the law in Belgium applies the exemption relating to the data subject being allowed to ‘put his point of view’ not only to (pre)-contractual circumstances but also to decisions based on a law, and the Greek law not only gives any person the right to put his point of view to such a decision, but also allows him to request from the court the immediate suspension or non-application of any act affecting him and that is based solely on such automated processing.

So far this provision has been applied extremely rarely. Even in France, where this system originates and an in-principle prohibition has been in effect for many years, there is no case-law on this matter. The French data protection authority has, however, issued

---

[13] This section is limited to the right to object to direct mailing: the right to object to direct marketing use of one's data for tele(phone)-marketing and marketing on the Internet are also subject to special Directives which are outside of the scope of this report.

guidance on credit scoring and by means of a recent recommendation as regards the collection and processing of personal data for the purposes of employment recruitment.[14]

9. Exemptions and restrictions (Article 13)

The Directive provides for a number of exceptions relating to major public interests for several of its provisions on the two conditions that such exemptions must be provided for in "legislative measures" and be "necessary", i.e. respect the proportionality principle, among others, to safeguard the public interest.

Processing in the areas listed in Article 13 (1) is often subject to separate legislation, and thus outside the scope of this analysis. This section thus only describes a number of exemptions that are foreseen in Member States' data protection laws.

Several Member States set out limitations for the matters and purposes foreseen in Article 13 with some of the laws stating that the application of such exceptions remains subject to supervision by the national data protection authority. For instance, the UK law stipulates in some cases that the exemptions only apply to the extent that the full application of the provision from which they allow derogations "would be likely to prejudice" the matters concerned. This means that the courts and the UK data protection authority are able to assess the necessity of any such exceptions and their application in practice, in accordance with the Directive but on a case by case basis.

The Greek law allows for restrictions on the exercise of data subject rights only for reasons of national security or if this is necessary to prevent or investigate "particularly serious crimes", and even then only provided that the controller (i.e. the security or police agency involved) obtains special authorisation from the Data Protection Authority.

The Finnish law already uses more limited exemptions than the Directive would allow and adds that the right of access applies "regardless of secrecy provisions" and that any controller relying on such an exception must issue a written certificate to that effect, and this certificate must mention the reasons for the refusal. The Luxembourg law takes a similar line and in addition requires that the data protection authority must be informed of the reasons for refusal. This should ensure that the exceptions are restrictively applied, in accordance with the Directive.

The laws in the Member States vary considerably in the wording used to express the need to protect the interests of data subjects and others, Art. 13(g) and the tests applied are quite vague. Some of the laws do not contain a general provision; it might be felt in those Member States that the ordinary rules and exceptions concerning specific matters were flexible enough anyway.

The other Member States' laws all contain an exception, or more specific exceptions, to protect data subjects or others, but they apply very different tests in this regard. Such range from mere balance tests or the need for an overriding interest of others in the

---

[14] Délibération n°02-017du21mars2002; see http://www.cnil.fr/frame.htm?http://www.cnil.fr/textes/recomand/d02-0171a.htm

German and Austrian laws, to very strict tests, as for instance in Denmark that requires an “overriding vital private interest” to trigger the exemption. The UK and Irish laws both contain more specific exception clauses than the protection of the data subject or of the rights and freedoms of others which reflect the view of the legislator on how the balance between conflicting interests must be struck in particular contexts. Thus, the UK law has a provision whereby access can be denied to “confidential references” given about job applicants and to personal data used in “management forecasts” or –“planning” and negotiations with the data subject to the extent that providing access to such information “would be likely to prejudice” the interests of the data controller. In Ireland, the law contains particular exceptions to subject access, for instance concerning in-house estimates of possible liability under claims made against the controller to the extent that providing access to such information “would be likely to prejudice” the interests of the data controller.

There is no certainty that these different tests will be applied consistently throughout the Community. On the contrary, they are likely to lead to further divergences. There are therefore again quite significant divergences between the laws in the Member States.

10. Confidentiality and Security (Articles 16 and 17)

The laws in all Member States stipulate the confidentiality and data security requirements set out in Articles 16 and 17 of the Directive, often in terms identical or close to those of the Directive. Some laws include additional stipulations in order to give more practicality to the security requirements, such as for instance that, within the organisation of the controller, access must be limited on a need-to-know basis. All the laws also stipulate that controllers have a duty to select a processor who offers sufficient guarantees of reliability and competence. The Finnish law makes a distinction as regards "professional" processors which tries to meet the concerns that the formal requirements of the Directive as regards the existence of a written contract may be excessive in certain cases (such as, for example, the processing of a membership list of a small local football club on the club's behalf by a member. Such a member, for example, would not be a "professional" processor.)

As regards the determination of the technical and organisational measures, most Member States have opted for a formulation similar to Article 17 of the Directive. In other words, most of the laws have imposed upon data controllers a general obligation of result rather than an obligation of setting up concrete security means. This is not the case, for example, in Spain where a detailed regulation determines with great detail those technical and organisational measures that should be in place in response to concrete levels of risk for the protection of fundamental rights and freedoms of individuals. The Netherlands, have also approved detailed security measures which are not binding on data controllers although widely used on a self-regulatory basis.

Another aspect related to Article 17of the Directive is the issue of Privacy Enhancing Technologies (PETs), although some other parts of the Directive also refer to this

concept[15] . The Commission is therefore convinced that there is no need for amendment of the Directive to include an article on privacy enhancing technologies.

The concept of PETs aims at organising and / or engineering the design of information and communication systems and technologies with a view to minimising the collection and use of personal data and hindering any unlawful forms of processing by, for instance, making it technically impossible for unauthorised persons to access personal data, so as to prevent the possible destruction, alteration or disclosure of these data. The practical implementation of this concept requires organisational as well as technical solutions. Several PET strategies are commonly known, such as PETs in the classical sense - technologies that aim at accomplishing the largest possible use of truly anonymous data-, technologies aiming at the promotion of lawful processing, taking into account all the principles of the Directive and aiming at preventing all possible forms of unlawful processing, and thirdly a combination of both strategies.

Two countries, the Netherlands and Germany, have included an article referring to privacy-enhancing technologies in their data protection legislation. The German federal law foresees that additional legislation be passed on data protection audit, laying down detailed requirements related to the examination and evaluation and the procedure, selection and approval of the experts carrying out the audit. Some data protection authorities like the ones in the Netherlands and in the Land of Schleswig-Holstein in Germany have taken a very active role in the promotion of PETs, which has lead to the development of interesting measures for instance in the field of certification and auditing in both countries that are very suitable means to push and promote the advantages of PET. In Schleswig-Holstein, for instance, a regulation concerning audits and privacy seals exists. Companies can have an audit done by the authority on a voluntary basis but financed by the controller. The results of the audit can be used by the company as positive publicity, which is an incentive for companies. The criteria for the seal of quality are both legal and technical, it should be altogether adequate for the user. The seal is valid for two years, after this it has to be obtained again. Companies can present a written report done by an independent expert to the authority that checks it and verify the results. Experts need to go through an accreditation process if they want to be qualified to write these reports. It is therefore a very interesting example of co-operation between the private and the public sector. The Dutch authority offers a so-called PET scan for companies who could like to have assistance assessing the level of technological protection offered by their own processing. This technique has been successfully used in the private and public sectors.

---

[15] For instance Article 6 that embodies the principle of data minimisation in its letter c) by stating that the processing of personal data must be limited to data that are adequate, relevant and not excessive. This idea is further reinforced by its letter e) that adds that data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Recital 46 of the preamble to the Directive stresses the fact that the protection of the rights and freedoms of the individuals with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself.

11. Notification and publicising activities (Articles 18-21)

The system of notification and prior checks as set out in the Directive responds to the essential principle of transparency and efficiency of control in that notification is required, in principle. Member States may, however, provide for the simplification or exemption from notification where it is deemed unlikely that the rights and freedoms of data subjects are adversely affected. On the other hand, they have to foresee prior checks for operations that are likely to present specific risks to these rights and freedoms. This system reflects the different tradition in Member States, whereas some rely heavily on notification, others seek to minimise these.

Following the Directive, all the Member States, in principle, require notification of all wholly or partly automated processing. In most Member States, notifications must be submitted to the national data protection authority.

Some Member States foresee the duty to notify processing operations to all processing of personal data, including those held in manual filing systems (Denmark, Greece, Italy and Luxembourg), while some extend it to only some of the manual systems (Finland and Portugal). As regards the content of notifications, the national laws include all the matters listed in Article 19 of the Directive, with many laws stipulating further notifiable particulars[16]. In fact, only the Swedish law limits the particulars to those contained in the Directive.

---

[16] The Italian law adds the location of the processing, details about any processor, and details about interconnections to the list. The Luxembourg law requires notification, more generally, of the "condition" (i.e. the "criterion") on which the lawfulness of the processing is based, as well as of the period of retention of the data. The Belgian law stipulates that controllers must include information on the measures they take to inform data subjects of the various matters of which they must be informed, and on the way in which data subjects can exercise their rights. The law in Denmark demands that controllers add a "general description" of their processing operations, including the dates on which the processing started and when it is expected to end. The Greek law also requires information about the period for which the data will be processed or retained, while the French and German laws require notification of the retention period of the data. The Finnish law demands that, if fully automated "significant" decisions are taken by the controller, he must include the "logic" used in his notification, and also stipulates that controllers must notify the data protection authority of the measures which are taken within the controller's business for monitoring the use of the personal data files. In Portugal, controllers must notify the circumstances in which data may be disclosed to the recipients mentioned; details of any processors involved in the processing; information about combining (interconnecting) of personal data processing; the facilities and formalities provided with regard to the exercise of data subject rights; and (as in several of the above-mentioned States), the length of time for which the data are retained. In Spain, the law adds that the location of the processing system concerned must be mentioned in notifications made by private-sector controllers (as concerns processing by public-sector controllers, the details published in the Official Gazette must include the purpose of the file; the categories of the system and a description of the personal data to be included in it; any intended disclosures and/or transfers to third countries of the data; the officials in the relevant administration who are responsible for the system; the departments or units to which data subjects should turn if they want to exercise their rights with regard to the systems concerned; the security measures taken; and details about the retention of the data). By contrast, the notifiable particulars listed in the Swedish law, and under the proposed new Irish law, are limited to the basic particulars listed in the Directive.

In some countries, such as Greece, the law specifies that matters for which a "prior check" or "prior authorisation" is required must also be mentioned on the notification form - presumably, so that the authority can notice that the controller in question should comply with such further-reaching formalities.

Several Member States provide for many exemptions. Austria[17], Belgium, Denmark, France[18], the Netherlands[19], Italy, Sweden, Finland and the United Kingdom[20] all make more or less extensive use of the possibility to grant exceptions.

Germany, the Netherlands, Sweden and Luxembourg are the only countries that foresee the appointment of data protection officials[21]. There is an obligation, in principle, under German law for all bodies that collect, process or use personal data by automated means to appoint a data protection officer[22] The consequence is that notification is then not required anymore; the officer must maintain a register of processing operations

---

[17] The Austrian law fully exempts processing of published data, data from public registers, anonymised or psedonymised data and data processed for the purpose of publication from notifications. The law also fully exempts processing operations that fall within so called standard operations issued in accordance with Art. 18 (2), 1st indent.

[18] In France, there are similarly 42 categories of processing operations for which "simplified norms" have been issued; the "simplified notifications" of processing relating to these categories comprise more than 70% of all processing notified to the data protection authority. The law does, however, not contain a possibility to totally exempt processing operations from notification.

[19] In the Netherlands, exemptions have been issued for the processing of data on membership in ordinary associations, foundations etc., membership of religious or philosophical associations, personnel data and salary administration and related matters (such as redundancy, retirement and pensions), accounts data, data on job applicants, temporary workers, suppliers, landlords and tenants (and others hiring and hiring out goods), the processing of data on clients by lawyers, legal advisers and accountants, or by carers or care homes, or relating to child care or education (i.e. student data but also data relating to student transport, or to former students), data relating to permits and licences etc. issued by public authorities, local taxes and duties for graves, travel documents (passports), naturalisation (the acquisition of Dutch nationality) and changes of names, military service, archives and the keeping of records or documentation, personal data used in scientific or statistical research (which includes market research), intranets, computer systems and internal communication systems, video surveillance and other supervision over access to premises, data on visitors, other internal management data, the handling of complaints and legal proceedings, certain name-and-address lists and lists of a company's own customers for the company's own communications to those customers. In Portugal, simplified norms have been issued with regard to staff salary- and similar payments; data on library and archive users; invoicing and management of contacts with clients, suppliers and service providers; administrative management of staff, employees and service contractors; records of persons entering and leaving premises; and collections of subscriptions by associations and contacts with their members.

[20] The UK exempts just four types of processing operations: processing for the purpose of staff administration, for the purposes of advertising, marketing and public relations, for the purposes of keeping accounts or records, and processing which is carried out by a not-for-profit body or association.

[21] In the UK, the law expressly foresees the appointment of data protection officials. Arrangements have to be made through an order. No order has yet been made.

[22] As an exemption, non-public bodies are only bound to do so if they employ more than 4 persons in such activities. Companies where personal data is collected, used or processed by non-automated means, and where at least 20 persons are employed for that purpose must also install a data protection officer.

containing the information that would have had to be made in case of notification. The appointment can be made in the person of an employee or an outside expert. The Dutch law too places particular emphasis on this institution, the officials can be appointed either by a particular controller or by a (sectoral) organisation to which controllers belong. The number of data protection officials registered at the DPA has recently exceeded a total of hundred and is still increasing. As a result, a national professional association of data protection officials has recently been established. The Luxembourg and Swedish laws, too, make provision for the appointment of an officer, and exempt controllers who make such an appointment from notification requirements; in Sweden in order to benefit from exemptions (but not from prior checking, where applicable), the appointment needs additionally to be notified to the data protection authority. The Belgian law foresees to establish a data protection official in some specific cases but does not determine status or competences. Moreover, a "conseiller en sécurité" exists under specific Belgian law. This "counsellor" appears to be rather advising on security matters, as the name suggests, and does not hold the necessary competences foreseen in Article 18 (2), 2nd indent, to be considered a personal data protection official within the meaning of the Directive.

By contrast, Spain has not availed itself of the possibility to introduce any exemptions at all from notification for innocuous processing operations Portugal has only exempted from notification those filing systems which contain publicly accessible information.

The point to be noted here is that - in spite of some similarities and parallels - the standards in the different Member States differ significantly in scope and detail. Even with respect to similar operations which, in different Member States, are subject to exemptions the norms are different. Companies which want to harmonise such operations throughout their different establishments in the EU will therefore often not benefit from such "simplified norms" or exemptions.

As regards prior checks, the system is most widely developed in France, where all processing operations in the public sector must in principle be based on a regulation adopted after the data protection authority has given its positive opinion which in practice comes close to an authorisation. There is no similar provisions as regards the private sector, instead, the law foresees a simple notification by the controller. 70 % of data processing, however, are covered by the regime of "simplified" notification. By contrast, no processing is made subject to a prior check in the UK to date (even though the law does provide for the possibility); and indeed, the data protection authority feels that no such checks should be introduced for any processing.

There are substantial differences between the Member States as concerns the kinds of operations for which they stipulate such prior formalities. In Austria, for example, prior check is required for processing for the purpose of credit referencing. This category is also subject to prior checking in Denmark which also adds to the list processing by staff recruitment agencies for example. In Sweden, to mention another example, prior checks have been stipulated with regard to processing sensitive data for research purposes without the consent of the data subject, unless the research has been authorised by an "ethic committee", and also with regard to certain types of processing in the field of criminal investigations and processing of personal data concerning hereditary disposition derived from genetic investigation. In Germany, processing of sensitive data and processing involving the taking of automated individual decisions require a prior check. That check is, uniquely, to be carried out by the data protection official rather than the authority as regards the private sector.

All the Member States provide for the establishment of a publicly accessible register of processing operations, containing all the notified particulars, except for details of the security measures taken by controllers, in accordance with the Directive (although of course, the contents of these registers will vary because of the differences in the notifiable particulars). In Spain for example, the register contains both the notified particulars with regard to private-sector controllers and the published particulars of processing by public-sector controllers.

It results from the reports of the data protection authorities that the register of notified particulars overall is used rather rarely. Indeed, there is evidence that, to the extent that the registers are consulted, this is mainly by competitors and persons or companies with a commercial interest, rather than by ordinary data users. This is in spite of the fact that the authorities have gone to considerable lengths to make the registers as easily accessible as possible, especially on-line. Thus, in France, the number of requests for an extract from the register more than doubled between 1995 and 2001- but in real terms, this still only meant that it rose from 122 to 252 *per annum*, i.e. to just about one request for each working day. New statistics from Denmark appear, however, to point to a much wider use of the register, with approximately 1,000 consultations per month.

12. Judicial remedies, liability and sanctions (Articles 22-24)

12.1 Article 22- Remedies

The existence and ready availability of effective remedies against unlawful or improper processing is essential to ensure both compliance with the law in general and enjoyment of the rights and remedies of data subjects in particular.

The Article 22 reference to judicial remedies is without prejudice to any *administrative remedy* provided under Article 28 by the supervisory authority. Article 22 instead contains a guarantee of access to the courts. All the Member States allow for such a possibility of data subjects to seek redress and corrective action through the courts.

The data protection authorities are not penal authorities[23] but often have an obligation to report offences against data protection law to the police, the competent Minister or Public Prosecutor (e.g. Austria, Italy[24], Spain[25], Denmark and the Netherlands[26]).

---

[23] Exception to this generalisation in Ireland, with the DPA in Belgium enjoying pre-trial investigative powers.

[24] For example in Italy in 2001, 7 persons were referred to judicial authorities because of failure to notify the Garante, because of unlawful processing operations and because of failure to take minimal security measures.

[25] In normal circumstances violations of the data protection law are investigated and sanctioned by the Spanish data protection authority in accordance with an administrative procedure. In exceptional circumstances, where the Spanish Authority considers that the facts under investigation may also constitute a criminal offence, it may report this fact to the Public Prosecutor.

12.2 Article 23- Liability

The Directive provides for the right of a person to receive compensation from the data controller for damages suffered as a result of an unlawful processing operation. Such compensation is granted irrespective of the controller's fault, but there is an exculpatory provision if the controller proves he is not responsible for the event giving rise to the damage. The Directive does not specify the type or quantum of compensation which is to be granted.

All the Member States allow for the possibility of data subjects seeking redress, and corrective action, including damages, through the courts. There are, however, differences in the scope of liability. Whereas in some Member States, the controller is liable for any kind of damage, material and immaterial, in others the law is more restrictive as concerns the latter. As regards the grounds for determining the controller's responsibility and exculpation, the Austrian law provides for responsibility only in case of culpable unlawful use of data, as opposed to the rest of Member States. All Member States avail themselves of the exculpatory provision, with some specifying the conditions for a controller to rely on this provision in the law itself and others applying the ordinary rules on civil and administrative liability.

To the knowledge of the Commission there are currently few claims made in practice, but should this change, the general nature of Article 23 means that there would be differences concerning the scope of liabilities borne by controllers.

12.3 Article 24- Sanctions

The Directive contains a general obligation of Member States to provide for suitable measures to ensure the full implementation of rights and obligations contained in the Directive, and thus to lay down sanctions to be imposed in case of infringements. Given that a measure of law enforcement is at stake, Member States are free to choose the appropriate means. The Directive does, however, foresee that they have to put in place sanctions without specifying type, severity or scope.

All the laws contain extensive penal provisions, making most actions contrary to the data protection law a criminal offence, punishable by fines or, in serious cases even by imprisonment. Member States have adopted somewhat different formal procedures. For instance, in the UK and Ireland, criminal sanctions are largely linked to 'enforcement notices' which can be issued by the data protection authorities, and which are subject to appeal[27], while other countries solely rely on denunciations of wrong-doers by the national authority to the prosecuting authorities, or allow the data protection authorities themselves to bring prosecutions. These differences reflect the different legal cultures in the Member States; they do not detract from the in-principle availability of penal sanctions in all of them.

---

[26] The obligation to report to the Public Prosecutor by the Dutch DPA only applies with regard to indictable offences. In addition Article 162(6) of the Dutch Code of Criminal Procedure permits the Dutch data protection authority to agree with the Public Prosecutor to limit the reporting of indictable offences.

[27] Under the UK 1998 Data Protection Act, the Information Commissioner is the main prosecutor authority for offences.

All Member States with the exception of Ireland and Denmark foresee administrative penalties in the legislation which in most cases are to be imposed by the national supervisory authorities. There are important differences both in the amount of these administrative penalties and in the use of them by the Member States.

13. International Transfers of Personal Data (Articles 25 and 26)

The Directive was one of the first international instrument to contain rules on transfers of data to third countries. Such rules were deemed necessary to avoid a circumvention of the protection offered by the Directive when exporting data and a possible re-import to the Community. The Directive thus establishes that transfers to third countries may take place only if the third country in question ensures an adequate level of protection (Article 25). There are exceptions to this strict principle in Article 26.

13.1 Article 25's principle of adequacy

The laws of almost all the Member States contain a provision that transfers to a third country may in principle take place only if that third country ensures an adequate level of protection as set out in Art. 25(1) of the Directive. The French law of 1978 does not refer to this issue; instead the data protection authority applies the Articles 25 and 26 of the Directive directly. In determining such "adequacy" the same matters are taken into account as are listed in Art. 25(2) of the Directive - with the Spanish law adding some other matters, such as reports issued by the Commission[28] and the Irish law referring to 'codes of conduct or other [sectoral] rules which are enforceable in that country or territory '. The Luxembourg law prohibits transfers of data to third countries which do not ensure a level of protection which is "adequate and ensures respect for the provisions of [the Luxembourg] law and regulations" - which could be read as requiring adherence, not just to a generally "adequate" law but to a law which in specific details corresponds to the Luxembourg rules. The same applies for Finland

The German law is somewhat ambiguous in this respect, by stating the in-principle prohibition rather indirectly in a series of provisions which would, at first glance, appear to deal mainly with transfers outside the scope of Community law- but it must be assumed that the in-principle prohibition also applies to matters within the scope of Community law. It should also be noted that the German law generally focuses on the "adequacy" or otherwise of the protection offered by the recipient in any "third country", rather than by the level of protection offered by the laws and regulations in force in that country.

13.2 The assessment of adequate protection

There are considerable differences about the involvement of data protection authorities in the taking of adequacy findings as well as the role of the data controller in such assessment.

---

[28] This reference to the "reports of the European Commission" seems to link the general issue of adequacy finding to the Commission decisions under Article 25 (6) of the Directive.

Only in three Member States, France, Portugal and Spain, may the national supervisory authority take adequacy findings with general effects on its own initiative, but even in these countries such findings have been extremely rare. Also in three Member States, Belgium, the Netherlands, and Sweden, the national supervisory authorities do not take such general adequacy findings but instead it is the Minister of Justice or the Government, although it is expected that they would consult the data protection authorities. In the remaining nine Member States neither the supervisory authorities nor the Governments are empowered to take any general adequacy findings about third countries. The general trend is that authorities or governments limit their role to confirming at national level the adequacy findings of the European Commission. Authorities rather deal with specific transfers that do not however imply a general decision on adequacy of a third country.

The Member States also take different approaches to the situation pending formal findings of adequacy by either their national authorities or the Commission. In Austria, Greece, Portugal and Spain the law makes clear that in the absence of a Commission finding, only the national authorities can determine that a particular third country provides adequate protection. In other words, until and unless such a domestic (or European) finding has been made with regard to a particular third country, transfers of personal data to that country may only take place on the basis of one of the specified derogations. The law is not that clear in this respect in Italy, in particular because transfers need to be notified to the Authority which may object to the transfer within 15 or 20 (if sensitive data are transferred) days and the situation in Belgium is unclear because of the lack of a Royal Decree that should serve to complete the legislation.

However, in the other countries it would appear that pending such a formal determination, individual controllers can make this assessment for themselves, and can therefore decide to transfer data to third countries with regard to which there is no formal domestic or European finding of adequacy, if they have come to the conclusion that the country in question ensures an adequate level of protection. This is formally stipulated in the Luxembourg law (which merely adds that "in case of doubt", the controller should seek advice from the data protection authority). The different approaches to this question pending formal findings therefore result in substantial divergences between the Member States.

13.3 The effects of adequacy findings of the European Commission

It may be added that the laws in Austria, Finland, Ireland, the Netherlands, Spain, Sweden, Portugal, Italy and the UK all expressly ensure that if and when the Commission does make a "finding of adequacy" under Art. 25(6) of the Directive, such findings are given effect domestically[29]. The Luxembourg law requires adherence to a Commission finding to the effect that a particular third country does not ensure "adequate" protection (Art. 25(4) of the Directive). In Denmark, Commission findings of this kind are adhered to in practice without further ado, which means that a special provision in the law,

[29] Adequacy decisions approved by the Commission are addressed to the Member States and are directly applicable without any implementing measures at national law necessary. The adoption of national measures however may result necessary from the internal perspective.

allowing for the implementation of EC decisions on the implementation of the Directive has not been used.

13.4 Article 26's derogations

Member States have generally closely followed the text of the provisions in Article 26 of the Directive, however, with several laws considerably departing from it.

To start with, in Austria the law is strict as concerns transfers in connection with a contract, in that it says that data may only be transferred if clearly in the interest of the data subject and the contract cannot be performed without a transfer. It adds that transfers to protect the vital interests of data subjects or important public interests may only be made without a permit if the matter is so urgent that there is no time to obtain a permit, and that the data protection authority must be informed of such exceptional transfers forthwith. Data may be transferred where they are necessary in connection with the exercise of " legal rights before foreign authorities" and even then only provided they have been lawfully obtained. The law furthermore does not exempt transfers of data from public registers from the permit-requirement and does not contain the derogation on public registers provided for in the Directive. On the other hand, the law adds derogations in respect of transfers of information which have been "lawfully published in Austria", in respect of "indirectly identifiable data" and transfers specifically envisaged in (read: authorised by) an Austrian law.

The law in Spain contains a derogation which only refers to the public interest, rather than to an important public interest, to which it adds that transfers "requested by a tax or customs authority" in any country without "adequate" (or indeed any) data protection "shall be considered as meeting this condition." The law also contains a special derogation concerning processing "related to money transfers", provided the data transfer is in accordance with special legislation on such transfers.

The law in Ireland lists as the first derogation transfers of data which are "required or authorised by or under any enactment or required by any convention or other instrument imposing an international obligation on [the Republic]". Part of this can be said to be covered by the derogation contained in Art. 26(1)(d): transfers which are "necessary or legally required on important public interest grounds"- but transfers which are merely "authorised" (i.e. permitted) on the grounds mentioned are not necessarily "necessary or legally required" for the purposes mentioned. As far as the first derogation mentioned in the Directive is concerned, the Irish law fails to stipulate that "consent" for a transfer to a country without "adequate" protection must be "unambiguous". The law also extends the derogation concerning transfers needed to protect the "vital interests" of data subjects (Art. 26(1)(e) of the Directive) to transfers which are "necessary to prevent injury or other damage to the health of the data subject or serious loss of or damage to property of the data subject or otherwise to protect his or her vital interests", in cases in which "seeking [the data subject's] consent to the transfer is likely to damage his or her vital interests".

The laws in Greece and Italy also add the proviso to the derogation concerning transfer of personal data to protect the vital interests of the data subject that this derogation only applies if the data subject is (legally/mentally or physically) incapable of giving his or her consent to the transfer. The Greek law limits the derogation to protect important public interests to cases in which there is an exceptional need.

The general data protection law in Sweden itself also does not contain a derogation with regard to data obtained from a public register- however rules on the export of data from public registers are contained in the special laws or regulations on such registers. As far as the important "SPAR" register is concerned -which contains data on all Swedish citizens- the special rules on public access to official documents in effect apply the derogation envisaged in the Directive.

13.5 Transfers by adducing adequate safeguards (Article 26 (2))

All but one of the laws of the Member States provide for the possibility of allowing transfers on the basis of safeguards resulting from contractual clauses.[30] The only country in which this is not expressly done is Greece although in this country (as in Portugal) all data transfers are subject to authorisation. Most of the Member States have not taken major steps in this regard at the domestic level, because of the efforts being made at various international fora, and by the European Commission. Exceptions are the Netherlands and Spain, where the Data Protection Authorities have issued papers on international transfers which include a list of matters to be addressed in such contracts. In France, the data protection authority has been asked to review contract clauses drafted by companies on many occasions[31].

13.6 Effects of the Commission Decisions on Standard Contractual Clauses (Article 26.4) and duty to notify national authorisations pursuant to Article 26 (2) (Article 26.3)

By virtue of Community Law, these Commission decisions take full effect without any implementing measures at national level being necessary. Three countries (the UK, Portugal and Finland) have nevertheless foreseen in their laws the effects of Commission decisions pursuant to Article 26 (4) of the Directive. The European Commission has until now approved two decisions on standard contractual clauses.[32]

As regards Article 26 (3) of the Directive, that is, the duty to notify the European Commission of any authorisations granted pursuant to Article 26 (2) on the basis of sufficient safeguards adduced by the data controller, such an obligation is only contained in the laws of Denmark, Portugal, the Netherlands, UK and Austria. Those countries have notified to the European Commission a rather low number of authorisations. Although such a duty is not provided by the national laws, the European Commission has also received several notifications from Spain [33], Finland, and Germany. The extremely low number of notifications indicates either that Member States have failed to notify

---

[30] Despite the text of the law, the national supervisory authority in the United Kingdom has been reluctant to authorise any transfers and it has indicated that its role is limited to providing guidance regarding transfers. There are some indications that the Information Commissioner might change this approach in the future.

[31] Some 200 requests have been made to date, covering about 50 draft contracts

[32] Decision 2001/497/EC of 15 June 2001 and Decision 2002/16/EC of 27 December 2002.

[33] Some of them were notified even before Spain notified implementing measures to the Commission in the year 2000.

authorisations to the European Commission or that Member States are not granting authorisations as provided for in Article 26 (2) of the Directive and national laws transposing it.

14. Codes of Conduct (Article 27)

Article 27 provides for the possibility of drawing up self-regulatory codes of conduct, which are seen as a useful means to clarify the application of data protection law in a particular sector. The bottom-up approach ensured by self-regulatory mechanisms should increase the awareness among data controllers of the existing rules as well as their willingness to comply with these.

14.1 Community or National Codes?

Article 27 makes reference to both national codes and Community Codes. A distinction may be noted between the paragraph concerning Community Codes, which envisages the "approval" of such codes and the paragraphs concerning national codes, which refer more vaguely to the obtaining of an "opinion". In most Member States, the laws refer to the "checking" or "assessing" of the compatibility of the code with the law and/or to the issuing of an opinion on that conformity. However in Luxembourg the law refers to the "approval" of codes by the national authority, using the same language as for the "approval" of Community-wide Codes by the Article 29 Working Party.

14.2 Content of national Codes

National codes cover a range of areas with issues like direct marketing addressed or in the process of being addressed in several Member States. To mention some examples, the Italian data protection authority has drawn up codes of conduct for journalists and historians, with work on codes for statisticians, defence counsel and private detectives being finalised[34]. The German Federal authority contributed to the development of a code of conduct for the protection of personal data in editorial offices, which was then elaborated by the Presserat (the self-regulatory supervisory board for the press). The Dutch authority has approved many codes of conduct and is presently involved in the development of codes of conduct in various fields such as scientific research, market and policy research, banks and insurance companies, trade information offices and recruitment agencies.

---

[34] In the near future the following codes will also have to be adopted in Italy in pursuance of Section 20 of legislative decree no 467/2001, as regards the processing of data a) that is performed by providers of communication and information services offered via electronic networks ; b) that is required for social security purposes or in connection with the employer-employee relationship c)that is performed for sending advertising material and/or for direct selling purposes, or else to carry out market surveys or interactive commercial communication activities ; d) that is performed for commercial information purposes e) that is performed within the framework of information systems owned by private entities, where they are used to grant commercial credits or else concern data subjects' reliability and timeliness in performing payments ; f) that is included in archives, registers, lists, records or documents held by public bodies ; g) that is performed by means of automated image acquisition devices. Compliance with the provisions set forth in the above codes will be a fundamental prerequisite for the processing to be lawful.

In France the professionals concerned generally ask the CNIL for opinions and so the CNIL serves as a advisor of the draft code of ethics before any final adoption. These professional initiatives lead the Commission to start detailed co-operation with the professional organisations concerned. The code projects and the official opinion of the CNIL on their conformity in the law are systematically examined at a plenary sitting. To the knowledge of CNIL, no code of ethics or good practice has been implemented of which it has not been asked to advise beforehand, even though such a referral to the CNIL is not obligatory.

The law in Spain allows for the possibility of single organisations (such as groups of companies, or even one company, or a single government department) adopting a code, and submitting it for assessment. So far the Spanish Authority has approved nine codes of conduct dealing with issues such as telecommunications, e-commerce, solvency and credit or advertising on the Internet.

Under Finnish law, controllers or their representative organisations may compile sectoral codes of conduct for the application of the Data Protection Act and the promotion of good processing practice, and may submit the said proposals to the Data Protection Ombudsman. The Data Protection Ombudsman may check whether a code of conduct complies with the said Act and with other provisions governing the processing of personal data.

The laws in several Member States show features, which reflect the trend towards *quasi-self-regulation*. Thus, the law in Denmark refers to the drafting of codes by sectoral associations "in co-operation" with the data protection authority. In Spain, the data protection authority may enter a code, which the authority regards as in conformity with the law, into the Data Protection Register. This lends the code considerable weight - but if the authority feels that the draft code is deficient, it must demand that changes be made. In Italy, the law requires that the organisations of the press adopt their own code, as they have done - but if they had failed to do so, one would have been imposed on them.

In Greece, the authority generally prefers to rely on the issuing of its own sectoral rules (rather than leaving the initiative, at least initially, to the sectors concerned) and in some other countries some specific sectors are already regulated in some detail in the law or in regulations issued under the law (e.g., the direct marketing- and credit reference sectors in Denmark). Elsewhere the possibility of issuing national sectoral rules is regarded more as something to be used only if a sector does not itself put forward adequate rules.

Community Codes

One of the first documents approved by the Article 29 Working Party (1998) [35] set up the procedure for the Working Party to handle requests for Community codes. At the time it was expected that the Working Party would have to deal with many such requests, which,

---

[35] See WP 13: Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct (working document adopted on 10 September 1998).; at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp13en.pdf

however, proved untrue. Up to now only three organisations (FEDMA- direct marketing, AESC- head-hunters and ETP- calling line identification) have submitted codes that fulfil the formal requirements of article 27 of the Directive and one (IATA) submitted a text that did not qualify as code under article 27 but received a rather positive opinion from the Working Party.

43% of the data controllers that responded to the on-line consultation felt that companies and DPAs have not made proper use of the possibilities offered by Article 27 of the Directive (i.e. codes of conduct) both at national and Community level with only 12% being of the opposite opinion. It is indeed disappointing that so little initiatives have been presented by industry to the Article 29 Working Party and that no Community code has been adopted up to now.

One of the difficulties associated to this article is that, while the aim is the adoption of Community codes, it says that the Article 29 Working Party has to judge the conformity of the code not against the text of the Directive but against the national provisions implementing it. The 1998 document of the Working Party 29 on the procedure for adoption of the codes interpreted this article as meaning compliance with the Directive and the national provisions but still, and given the existing differences in the implementation of the Directive at national level, this mention of the national provisions can complicate the process.

The little experience existing shows that the process for obtaining an "opinion" or assessment of the Working Party is long. This could maybe be explained by the fact that this is a rather new figure, not existent before the Directive, that therefore requires some pilot work being done but the more practical explanation relates to the fact that the organisations that have submitted draft codes up to now are composed by an extensive group of members of different nationalities and different backgrounds that need to be consulted every time amendments to the draft are proposed and this is very time-consuming. The work on the side of the Working Party 29 also requires time as the subgroup dealing with the draft code needs to report to the plenary and get their agreement and input before getting back to those who have submitted a code. It is expected that experience will help speeding up the process in the future.

The code of FEDMA, the European Federation for Direct Marketing in Europe is expected to be approved in the spring of 2003. This code deals with a number of significant issues in the direct marketing sector such as the collection of data for direct marketing purposes, explaining in detail the different possible situations; host mailings, disclosure of lists, the source of the data and so forth; the right to object to the processing for direct marketing purposes and particular issues such as preference services systems and in-house suppression lists. The code includes specific provisions on the protection of children, dealing in particular with the cases in which data are provided by children in order to participate in a game, to obtain a prize or a similar promotional activity. The last chapter of the code deals with compliance and monitoring, explaining the role that the national Direct Marketing Associations (DMAs) have to play concerning the application of the code and the resolution of complaints.

15. Supervisory Authorities (Article 28)

The establishment of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of personal data[36]. The Directive thus requires Member States to assign a wide range of tasks to the authorities. The roles they have to play accordingly range from ombudsman, auditor, consultant, educator, policy advisor, negotiator, enforcer to international ambassador. The first role, as perhaps the most classical one, is essential, although there seems to be an evolution towards an increasingly pro-active rather than a reactive role.

15.1 Status of the data protection authorities' independence

The Directive says that the data protection authorities must "act with complete independence" - which is meant to emphasise that they must not only be given formal independence but must also be free from interference in practice. Although no single formula exists, a number of elements do contribute to safeguarding the independence. Such elements include the composition of the authority, the method for appointing its members, the duration of exercise and conditions of cessation of their functions, the allocation of sufficient resources to the authority and the adoption of decisions without being subject to external orders or injunctions. These elements are also mentioned in the explanatory report to the additional protocol to Council of Europe Convention 108.

The laws in most countries do indeed stress that the authority "shall be an independent authority" or "shall not be subject to any directions in the exercise of its functions". In Germany, the situation is somewhat particular as regards the supervision of the private sector[37]. This sector is subject to unified substantive rules in the federal data protection law, but the Länder are competent to determine the supervisory authorities. Thus, in several Länder, the competent authorities are part of the Ministry of Interior or the Ministry of Interior and the regional government as subordinate authorities of the respective Land[38]. As such the regional government is fully subject to ministerial instructions while the Ministry itself is not subject to governmental instructions. In others, it is the Landes-data protection authority that is charged with supervising in respect of private-sector processing too, but the Ministry retains control of lawfulness or even lawfulness and appropriateness[39].

As regards the allocation of sufficient resources, many national supervisory authorities are of the opinion that they clearly lack such resources to fulfil the tasks attributed to them.

---

36 See recital 62 of the Directive.

37 For supervision of the public sector, the federal data protection authority is competent, with responsibility for supervision over processing by the federal authorities; and separate Landes-data protection authorities, responsible for supervision over processing by the public authorities of the Länder.

38 This is the case in 10 of the 16 Länder: Baden-Württemberg, Brandenburg, Mecklenburg-Vorpommern, Saarland, Bavaria, Saxony, Rhineland-Palatinate, Thuringia, Hessen, and Saxony-Anhalt.

39 The latter ('Fachaufsicht'-Kontrolle der Recht-und der Zweckmäβigkeit) in Lower Saxony, North Rhine- Westfalia, Hamburg and Bremen.

15.2 Tasks and powers of the authorities

Member States have generally granted the wide range of powers that the Directive foresees, although some notable exceptions are set out below.

Investigative powers (28.3. first indent)

All data protection authorities are charged with investigating possible breaches of the law within their jurisdiction. Such investigations can arise, in particular, out of doubts about a proposed processing operation as described in a registration form, or out of specific complaints from individual data subjects. Many data protection authorities also select particular issues or sectors for particular attention in a given period. Perhaps with the exception of Spain where there are hundreds of audits per year, relatively few audits are however been carried out by the other authorities[40].

Investigations, when they are carried out - and in particular the investigations into selected, important issues - are extensive, detailed and in-depth. All aspects of the processing operations in question are looked at and discussed with the data users, and precise and detailed views and opinions expressed on how the law is to be applied to them. In the Netherlands, the authority has started to carry out extremely detailed "privacy audits" of selected data users, again to ensure that all relevant matters are closely examined. In the UK the data protection authority cannot carry out such audits without a controller's agreement.

In most countries the national authorities are vested with extensive powers of access to files and filing systems used to process personal data, and the authorities can therefore usually demand full access to all relevant sites and materials. In the UK, however, the Information Commissioner can access the premises of companies only with their express permission or with a warrant.

Powers of intervention (Article 28.3 second indent)

Disparities between Member States laws are considerable in this regard. In some cases national supervisory authorities have not been given the powers foreseen by the Directive.
Many authorities hold the power to order the blocking, erasure and destruction of data and the power to impose a definitive or temporary ban on the processing. This is, however, not the case with the federal German, Belgian and the French[41] authorities, and neither the Italian nor the Swedish[42] nor the federal German authorities have the power to order the erasure or destruction of data.

---

[40] See, for instance figures in the report approved by the Complaints Workshop in Dublin, 14 and 15 March 2002, 'Information on the powers of European Data Protection Authorities (DPA) concerning request for information put to a controller, complaints, audits and sanctions, and on their implementation'.

[41] Under the present law the CNIL holds the power to impose a temporary ban on the processing only in exceptional circumstances

[42] It may then apply at the County Administrative Court.

Most of the authorities have the power of warning or adminishing the controller. The issuing of warnings or admonishment could be very helpful in those circumstances where authorities would like to take a more conciliatory approach as described above.

The law in most countries provide for the imposition, by the national data protection authorities, of a range of formal sanctions seeking to force data users to comply with the law.
Criminal prosecutions are generally extremely rare, reserved for the most obstinate law breakers such as companies which continue to maintain unregistered databases in spite of repeated warnings, or export data in spite of such warnings or formal notices, or people who knowingly flout the law by selling confidential personal information. However the authorities in many Member States are not penal authorities[43] but often do have an obligation or practice to report offences against data protection law to the police or Public Prosecutor (e.g. Austria, Italy[44], Spain, Denmark and the Netherlands). In addition, in many countries, the Authorities can impose administrative fines. However, such formal actions are, *in practice*, used only as a last resort[45].

The power to engage in legal proceeding or to bring these violations to the attention of the judicial authorities (Article 28.3 third indent).

As was already acknowledged by the twofold way this power was drafted in the Directive, differences between Member States in this area were and remain important.
Some authorities are bodies that prosecute and where appropriate sanction the violations of the law with no referrals to the courts (except for the denunciation of penal violations or in those cases where the offender would like to challenge the decision). This is the case for example in Spain or Italy.
Some authorities just have the power to investigate and to bring the violations to the attention of the judicial authorities. In some cases they may be part to the proceedings (e.g. Austria), while in some cases they may not.

The duty of hearing claims (Art. 28 (4))
The answers provided by the data protection authorities[46] have made clear that for some authorities the expression "to hear claims" does not necessarily mean the opening of an administrative procedure that is closed by administration resolution further to a data subject's complaint, whilst for others this is a normal practice.

---

[43] Exception to this generalisation in Ireland , with the DPA in Belgium enjoying only pre-trial investigative powers with no right to impose sanctions.

[44] For example in Italy in 2001, 7 persons were referred to judicial authorities because of failure to notify the Garante, because of unlawful processing operations and because of failure to take minimal security measures.

[45] With the exemption of Spain and Portugal.

[46] The following was the question put to the authorities- 18) Does the obligation of "hearing claims" as provided for in Article 28 (4), first paragraph, of the Directive entail the data subject's right to request the opening of an administrative procedure which is closed by an administrative resolution? In other words, is the opening of an administrative procedure at the discretion of your authority even if you have received a complaint from an individual? In case of affirmative response, we would appreciate to knowing what are the criteria on the basis of which your authority takes such decisions?

Several authorities consider that the data subject should always contact the controller first. The Information Commission in the United Kingdom has also developed an assessment handling system which contains some differences from the systems in place in other Member States.

16. Final Provisions (Articles 32-34)

Derogation under Article 32(3)

Data kept for the sole purpose of historical research need not be brought into conformity with the general processing rules of the Directive as set out in Articles 6,7 and 8. This provision has been transposed directly into many Member States' laws with the safeguard that such data cannot be used for any other purposes. Often the legislator is forced to reconcile requirements pertaining to the drawing up of statistics, access of persons to the documents concerning them preserved by the public bodies or ensuring a public service mission and in a more general way the relations between the administration and the public subject to such administration. Other Member States like the Netherlands and Finland, have not applied the derogation provided for in Article 32(3). The German federal law intends to permanently store archive goods for scientific use while special rules apply to the files of the state security service of the former GDR of 1992, the so-called *Stasi* files[47]. Austria's Archives Act operates on a federal level and governs the right to preserve material of archival value. It exempts data from the erasure requirement only if they have been designated as having archival value and could not be used during the archive embargo. The UK safeguards provide that the data is not to be processed so as to support measures or decisions with respect to particular individuals and the data is not to be processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

[47] Here there is no fixed time for erasure, but instead very tight restrictions to the processing and use that are supervised by a high ranking and independent Commissioner. The Commissioner may disclose personal data for the use of research or political education if there is either consent of the data subject or a legitimate wide public interest. This is an area of ongoing debate.

Part two: Impact on the Internal Market

The impact of the Directive and transposition laws on the Internal Market is difficult to gauge in one respect because there have been no complaints regarding the obstruction to the free flow of data, nor are economic indicators available, nor has the Commission been forced to begin enforcement proceedings in this regard. The main objectives pursued by this Directive have indeed been met. However, the divergences set out in the first part of this analysis are an impediment to a truly harmonised framework and capable of creating problems for businesses operating on a multinational scale. There have been issues raised by industry, data controllers and data subjects on troublesome implementation or application of particular provisions of the Directive.

Such problems in the application might arise either from a wrongful transposition of certain provisions in Member States' laws, or from divergences that are, however, within the margin of manoeuvre the Directive leaves Member States, or, finally, from different practices in the interpretation of the laws, mostly by national supervisory authorities.

In general terms, a negative impact on the Internal Market, in the sense that the free flow of data as guaranteed by the Directive is unduly restricted, may originate where Member States do not transpose all grounds for processing or transfer, or where implementing laws contain exceptions that are not in accordance with the criteria set out in the Directive. Many such examples have been given in the analysis section of this analysis that need not be repeated here at length. This applies for instance to Articles 7 (the criteria for making data processing legitimate, 8(2) (the exemptions to the general prohibitions to process sensitive data) , 13 (general exemptions and restrictions on grounds of important public interests) or 26 (exceptions to the general prohibition of transfers of personal data to countries that do not ensure and adequate level of protection), to mention but a few.

Further to that, differences in the application of individual articles of the Directive are capable of creating specific impacts on the Internal Market. Where applicable, those are outlined below.

Given that **definitions** in legal texts are crucial, the divergences detected in Member States' laws can have significant effects on the application of the legal rules. Differing definitions of the same concept make compliance for companies operating and established in more than one Member State more cumbersome. This applies for instance to the definition of personal data with respect to the online context (IP addresses) and in the field of clinical trials (key-coded data), as has also been pointed out in some position papers[48]. As regards the information gathered so far on the issue of 'consent' the submissions agree that there is a need for a consistent and clear definition of consent throughout the Community. The Commission is aware that these issues require further clarification and/or reflection.

Several submissions from business associations further argue that the application of the Directive to legal persons, as has been chosen to do in several Member States, causes substantial problems for such companies.[49]

---

[48] See for instance papers submitted by Covington & Burling, IMS Health.

[49] See, for example submissions received from the International Chamber of Commerce (ICC), the

Many submissions from business associations see the necessity for a distinction between 'personal data' and 'professional data', with the latter either being exempted from the rules of the directive or subject to derogations under it[50]. Such a distinction, they argue, would not compromise the legitimate expectations of individuals yet at the same time would reduce burdensome compliance with the Directive. The European Commission does not share these views and is convinced that most, if not all, of the concerns raised can be tackled within the margins of the present Directive which provides for sufficient flexibility, reacting differently to different interests, without putting excessive burden on controllers. Moreover, Member States are bound by Convention 108 of the Council of Europe, which also uses a broad concept of personal data, including professional data. The Directive also makes a link to the Convention in Recital 11. Further to that, under the case law of the European Court of Human Rights on Article 8 of the European Convention on Human Rights, activities of a professional or business nature are included in the notion of 'private life'[51].

As regards the implementation of the first main rule of the **applicable law** provision (Article 4 (1)(a)), it is clear from the analysis that the kind of conflicts the Directive wants to avoid might arise in some circumstances. In the majority of cases, Member States' laws have however succeeded in properly reflecting the Directive. At times, this has only been achieved by using formulations that unnecessarily complicate the application of the laws in practice. The existence of conflicts of law remains for the time being as a possible consequence of incorrect transposition in some Member States. Such a conflict may occur for example where a law foresees (wrongly) its application to all processing activities taking place in that country, while the controller in question is established in another country of the Community where the law correctly follows the applicable law rule of the Directive. So far, the Commission is not aware of any practical case in the Member States, probably because of the limited experience with the implementation of this provision and the fact that most of the time the national provisions implementing Article 4 a), paragraph one are considered only from the national and not a transborder perspective. The analysis of the second main rule of this applicable law provision shows that especially the criterion 'equipment' is difficult to operate in practice,[52] as is confirmed by the opinion of the Working Party 29 on Article

---

European Privacy Officers Forum (EPOF), the National Association of Insurance Companies (ANIA) or the

Federal Association Information Economy, Telecommunications and New Media (BITKOM).

[50] See, for instance submissions by Citibank, Union of Industrial and Employers' Confederation Europe

(UNICE), Association of Executive Search Consultants (AESC) or Confederation of British Industry (CBI).

[51] See, for instance the Niemietz v. Germany judgment of 16 December 1992, Series A, no 251-B, para.

29, Amann v. Switzerland judgment of 16 February 2000, *Reports* 2000 II, para 65; or, more recently, the

judgment Rotaru v. Romania of 4 May 2000, *Reports* 2000-V, para. 43.

[52] The difficulty in the application of 4 (1)(c) was a firm conclusion made by the rapporteur of the first

workshop of the conference on the implementation of Directive 95/46/EC, Rosa Julia Barcelo, and was

confirmed by other contributors throughout the conference.

4 (1)(c)[53] and the answers that Data Protection authorities gave to the Commission's questionnaire. This entire provision is subject to requests for revision in a majority of submissions received from industry and business associations[54]. In general, business finds it cumbersome to comply with this provision, especially as regards Internet issues and suggest the adoption of a country-of-origin rule. Most submissions from the US ask to introduce the country-of -origin principle also for non EU-based controllers[55]. Most also agree that the presence of equipment on EU territory should not be grounds for determining the applicable law. The Commission is not convinced that the adoption of a country-of-origin rule for non EU based controllers can be regarded as a valid alternative to the concerns to which this provision of the Directive responds . In the words of the Working Party 29[56]:

'The national laws of these third countries are not harmonised, the directive is not applicable in these countries and the protection of individuals with regard to the processing of their personal data may therefore be missing or weak. The country of origin principle, which is linked to the establishment of the controller, can no longer serve the purpose of determining the applicable law. It is necessary to switch to another connection factor.'[57]

From this follows that the introduction of a country-of-origin principle to such processing operations would result in very different, and weaker, levels of protection and is therefore not feasible. It is, however, essential to further clarify this provision, taking into account further technological developments.

The **principles and criteria** for making processing legitimate are at the core of the Directive. The divergences found in Member States' laws are therefore a particular impediment to a harmonised framework and create problems for businesses operating on a multinational scale.

The submissions address Article 7 rather than Article 6 and complain that there is a lack of consistency in the transposition laws, in particular with regard to the implementation of the crucial notion of 'unambiguous consent' in Article 7 (a) of the Directive. The submissions are, however, ambiguous here, in the sense that some rather want the notion

---

53 Art. 29 Working Party, Working Document on determining the international application of EU data protection law to personal data processing on the internet by non-EU based websites, WP 56 of 30 May 2002

54 To name but a few, C&W (Cable & Wireless), EPOF (European Privacy Officers Forum), EPC (European Publishers Council) or LIBA (London Investment Banking Association).

See, for instance, Global Privacy Alliance (GPA) and EU Committee of the American Chamber of Commerce.

56 Working Document on determining the international application of EU data protection law to personal data processing on the internet by non-EU based websites, WP 56 of 30 May 2002

57 Op. Cit, p. 8

removed, others want it more clearly defined. Other submissions propose the Directive should be based on a system that prevents abuse instead of regulating the use of processing[58]. The Commission can agree that such might be a useful and flexible concept for business although such an approach would bring about conflict with the provisions of other international instruments such as the Convention 108 of the Council of Europe, the European Convention on Human Rights and the Charter of Fundamental Rights. It recalls moreover, that the Directive already provides for a flexible framework in that there are extensive criteria under Article 7 to process data legitimately, and here especially under Article 7 (f) which contains a balance of interest criterion.

The divergences in laws as regards the **processing of sensitive data** result in different conditions in different Member States, an outcome the Directive aimed to avoid. 50% of data controllers who responded to the on-line consultation launched by the Commission were of the view that the existing rules on the processing of sensitive data are necessary, taking into account the risks for the privacy of individuals. This clearly shows that companies are well aware of the importance of a reinforced protection for these categories of personal data. 32% of those data controllers were of the opinion however, that determining the need to provide higher protection because of the sensitivity of the data should not rely on a closed list but on the effective risks for the privacy of individuals posed by the processing operation. 10% in the same study held that while the existing rules are necessary, their practical application is sometimes difficult.

The submission papers from Industry seem to be in favour of a uniform interpretation or a commonly accepted list of sensitive data. Some papers supported a treatment of sensitive data in much the same way as personal data; it thus would have to be determined in each particular case whether processing is fair[59] while others[60] preferred to focus on a 'protection from harm' principle. On a more specific level there was support for the inclusion under Art. 8(2) of a more comprehensive list of conditions justifying the processing of sensitive data to cover business sale, outsourcing, crime prevention, insurance and other situations[61].

The decision was made after long discussions to include in the Directive a list of data considered sensitive. The Commission wishes to recall that this is a closed list. It is the Commission's view that the Directive strikes a reasonable balance between the

---

[58] Such are, for example, the Dutch Council of Employers' Federations (RCO), the Clifford Chance or the

Swedish Union of Civil Servants (ST) with a view to the Swedish transparency principle that the directive runs

counter, in the view of ST.

[59] Paper by Clifford Chance UK, C&W (Cable&Wireless) and BBA (British Bankers' Association).

[60] Citigroup, Allen & Ovary and German Banking Association.

[61] Clifford Chance, Association of Commercial Information Agencies (Germany) and ACCIS

(Association of Consumer Credit Information Suppliers)supported the processing of data concerning offences

and criminal convictions.

protection of these special categories of data and businesses' interest in that the Directive is flexible enough to enable a processing of sensitive data and further to that grants wide possibilities for exemptions that Member States are free to use, under the conditions specified.

Divergences in the implementation of Article 9, although considerable, do not seem to have a significant impact on the Internal Market. A possible impact arises rather for the respective fundamental rights that Article 9 aims to balance. The main conclusion we obtain from a panorama of broad and important discrepancies between the Member States' laws is that where the laws foresee too little exemptions for processing **for journalistic** purposes, the right to freedom of expression as guaranteed by Article 10 of the European Convention on Human Rights (ECHR) risks to be violated, and where the laws foresee too wide exemptions, the individual's right with respect to the processing of personal data as guaranteed under Art. 8 of the ECHR, Convention 108 of the Council of Europe and recognised by Article 1 of Directive EC 95/46 might be unduly limited. As is always the case when reconciling competing fundamental rights, it is a question of striking the right balance with a margin of appreciation left to the Member States.

There are considerable differences between the laws in the Member States when implementing the **information requirements** set out in Articles 10 and 11 of the Directive and in particular, as regards subsection c) of both Articles 10 and 11. The fact that companies established in several Member States are faced with different legislation is, however, not an Internal Market issue *strictu sensu*, given that such companies are precisely not exploiting the Internal Market. A submission paper questions the necessity of certain categories of information, because they often create lengthy notices printed in small print that consumers tend to miss. The paper calls for notices that offer consumers information that is short, meaningful and actionable instead[62]. Indeed a significant element of the requirement to provide additional information to data subjects is the stipulation in the Directive that such information must be provided *when necessary for guaranteeing fair processing* to the individual concerned[63]. Standard notice forms may

---

[62] "Legally Mandatory Wording in Privacy Notices" , Hunton and Williams

[63] The results of the on-line consultation addressed to data controllers at this regard do not seem to indicate that making the provision of all or some of the additional information mentioned by the Directive compulsory for the controllers (e.g. Spain or Germany) leads to more provision of information to individuals than leaving the provision of this information to a decision by the controller on the basis of a necessity test (e.g. the United Kingdom). For example, only 54% of the German controllers and 46% of the Spanish controllers who admitted collection of personal data via the Internet inform the data subjects whether replies to a question are obligatory or voluntary despite of the fact that the provision of such information is a legal obligation in both countries. 33% of the British controllers declared to provide the same information only on the basis of a

be difficult to reconcile with the case-by-case approach the Directive establishes for the assessment of what further information is necessary to guarantee fair processing, although they may be useful both for business and data subjects.

Economic operators seem to share some misgivings about the Directive and national laws implementing it for possible refusals of **access** requests. They wonder, for example, whether or not a multinational company established in several Member States and with personal databases spread throughout the Community would be obliged to deal with an access request about any data of any individual which could be anywhere in the organisation within the EU. As a matter of principle, if the controller can retrieve the information for his own purposes, he should retrieve it in response to an access request. However, the Commission accepts the point made by four Member States (Austria, United Kingdom, Sweden and Finland) in their proposals for amendments that there may be a gap between law and practice regarding which data the data controller can actually locate. The Commission recalls, on the other hand, that access is a fundamental right of citizens, central to any data protection system and enshrined in the Charter of Fundamental Rights of the European Union. Thus, if the access request concerns "very hidden" information in the sense of information extremely difficult to retrieve and clearly excluded from the normal operations of the controller, the data controller may ask the data subject to assist the organisation in searching for his data[64]. The German law usefully stipulates in this respect that if a data subject approaches an entity which is part of a complex organisation or groups of organisations, the entity which is approached (e.g. a daughter company) must pass on the access request to other parts of the group as appropriate.

Some submissions from Industry have argued that the Commission ought to propose amendments to the Directive introducing a requirement of proportionality and justification for the right of access to improve "a current imbalance"[65] where industries are obliged to react to requests for access in bad faith[66] without any controls to prevent

---

necessity test. The similarity of the results is reaffirmed by the survey's indication that compliance with Articles

10 and 11 of the Directive is around a 10% higher in Germany or Spain than in the United Kingdom. The survey

shows that only 70% of the UK controllers who replied from the United Kingdom post information on their

websites as regards the purpose for which the data are collected and used (general obligation everywhere) while

80% of the controllers who replied from Germany or Spain declared to do so.

64 This assistance is already foreseen in the laws of the UK and Austria.

65 See, for example position papers from C&W (Cable&Wireless), ISPA (Internet Service Providers

Association) or DMA (Direct Marketing Association, UK).

66 See, for example position papers from UNICE (Union of Industrial and Employer's Confederation of

Europe) or CBI (Confederation of British Industry).

misuse[67]. The information gathered by the European Commission, however, seems to indicate, quite on the contrary, that the practical application of this provision generally does not amount to serious problems for companies. The answers provided by the data controllers to the on-line consultation support this assertion. First, 62% of the data controllers do not have a negative experience when responding to requests of access and their experience do not indicate that this activity involves an important effort for their organisations. Secondly, the number of request of access is extremely low[68] which appears to point to a lack of awareness among data subjects about the existence of this right.

As regards the **right to object** to direct marketing use of one's data, the information gathered so far indicates that the level of citizens' awareness is low. The extension of the right to object by some States to processing to which it does not extend in other States may, in practice, not make too much difference. However, the restrictions of the right in several Member States cause more significant difficulties. So far the exercise of this right has however been very rare and the experience of Data Protection Authorities is also very limited.[69] Differences in the implementation of the provisions on **automated individual decisions** do not seem to have any significant impact on the Internal Market so far, mainly because this provision has been applied extremely rarely in all the Member States.

The concept of **privacy enhancing technologies** is already an integral part of the Directive but the Commission realises that it is necessary to take additional measures to promote the use of these technologies. One clear proof of the fact that the application of these technologies is still too limited is the difficulties that some companies working in this field are experiencing; some commentators talk about a clear market failure in the sector due to the lack of sufficient demand by the potential users[70]. While one can never

---

[67] In particular here refer to the paper by the EU Committee of AMCHAM

[68] 396 of the respondents replied on behalf of organisations with more than 500 employees (40.2% of the total). Only 17 respondents declared to have had more than 500 access requests during the year 2001, while 40 respondents declared to have had less than 10 access requests and 28 between 10 and 50 requests.

[69] The questionnaire on the implementation of the Directive addressed to the Data Protection Authorities contained a question about the guidance provided by supervisory authorities in the Member States on the interpretation of the words "justified objection" in Article 14 a) of the Directive and national laws implementing this provision. Most of the national authorities have not replied to this question, others have acknowledged a lack of experience with the implementation of this provision (e.g. Spain) and others have not found reasons to issue further guidance (e.g. the Netherlands)

[70] See in particular the contributions of Stephanie Perrin and Lee Bygrave who referred to considerable but not insurmountable difficulties and to more obstacles than opportunities that make legal encouragement

be sure of which reasons have caused this situation, several possible motives could be pointed out:

- users are not sufficiently aware of the existence of these privacy-protective options and, even if they are aware, have difficulties recognising them. More awareness is needed as well as tools that could help the users identifying which technologies are privacy-enhancing and which ones are not.

- companies do not get sufficient advice at the moment of putting in place processing operations, that is the moment in which PETs can be built in without unnecessary expenses and delays. To that extent DPAs could play a more proactive role[71].

- often PETs are developed as tools that the user would need to use on top of other technologies implying additional efforts and expenses. In order to make PETs easily available to the users without expecting too much initiative from their side, they need to be integrated in existing technologies. The integration of PETs in existing technologies such as browsers or software packages would benefit both the users and the producers of these techniques.

- sometimes those using PETs that create domains of anonymity and pseudonimity are discouraged by the very extensive interpretation that some DPAs give to the concept of personal data that means in practice that the additional investment of financial and human resources is not rewarded. The interpretation of this concept needs to be clarified and applied in a reasonable way.

- governments might not have taken sufficient measures to promote PETs. As it is already the case in Germany and the Netherlands, governments could promote the use of PETs by using them themselves in their data protection activities like for instance in the e-government implementations.

There are considerable differences in the way Member States have approached **notification requirements**, although the number of notifications is generally astonishingly low when estimations are made of the number of companies and bodies which should in principle have notified their processing operations to the competent register[72]. These differences were already acknowledged by the Directive which set up an

---

indispensable.

[71] The Dutch DPA offers a so-called PET scan, for companies who could like to have assistance assessing the level of technological protection offered by their own processing. This technique has been successfully used in the private and public sector. See for more information the proceedings of the conference Privacy by Design, organised in The Hague in May 2002 (www.cbpweb.nl).

[72] The highest number of notifications can be found in France (700.000 files). It is interesting to note that the number of files is the same (around 250.000) in countries like Spain and the UK although they have taken completely different approaches towards notification: in Spain there are no exemptions to the duty of notification within the sense of Article 18 (2) of the Directive,while the UK has availed itself of these exemptions. In Ireland, there were 2.880 files notified in the year 2000, and in Portugal 3.832 during the same period.

open notification system. This does not make the divergences detected less undesirable, only foreseeable.

The review of the Directive has registered broad criticism towards the notification provisions of the Directive. Many called for a simplification of the notification procedure if not its abrogation given it raises huge administrative burdens that do not seem to add to protection for individuals[73]. This point was also made by data controllers who responded to the on-line consultation when they called for genuine protection of data rather than bureaucratic protection. There are also proposals to require notification only in limited circumstances, ensure that sanctions for failure to notify are proportionate and/or establish an EU-wide notification regime, a so-called 'one-stop-shop registration'[74]. Christopher Kuner at the data protection conference argued in favour of a strengthened role for company privacy officers and the subsequent replacement of notification requirements.

Some Data Protection Authorities and Member States, quite on the contrary, regard notification requirements as a very useful tool for many purposes, for instance in order to have an overview of processing operations, to verify compliance, consider complaints and increase awareness among data controllers. This aspect appears to be of particular relevance in the accession countries.

The Commission is of the view that the considerable differences detected in Member States make compliance cumbersome or might even discourage compliance. It recalls that the Directive already sets out a system that allows Member States to reduce notification requirements. Reducing discrepancies nevertheless does not mean adopting the less stringent approach as suggested by some. It means finding a balanced solution and implementing it throughout the Community.

As regards the provisions in the Directive on **international data transfers**, divergences between Member States laws are clear and numerous, despite a large measure of convergence as regards the general principles. It is in particular worth noting that Member States are divided in whether they require additional authorisation when use is made of EC decisions on adequacy or model clauses, and yet at the same time the number of authorisation requests is extremely low in the countries that require such authorisation[75]. This is a worrying combination as it seems to indicate that either data are

---

[73] For instance RCO (Council of Employers' Federation, the Netherlands), UNICE (Union of Industrial and Employers' Confederation of Europe), CBI (Confederation of British Industry) or ICRT (International Communications Round Table).

[74] This was raised by Clifford Chance, C&W (Cable&Wireless), Covington&Burling and the UK Direct Marketing Association (DMA).

[75] From zero (in a country that has implemented the Directive) to 11, with the authorisation procedure taking two months on average. Numbers taken from the Complaints Workshop's paper on transborder data flows.

not transferred, or that they are transferred without respecting the conditions set out in national legislation. Such divergences are likely to hinder the Community wide level playing field intended by the Directive when it comes to making business, and transferring personal data to that effect, with economic operators in third countries.

Those submissions that address the international transfer issue seem to agree that there is a need for clarification of several issues, such as who should be responsible for assessing adequacy[76], or guidance, for instance on the notion of 'unambiguous consent' or the requirement that transfers are 'necessary' for the conclusion of a contract[77], both in Article 26. Many submission also point out the importance of a uniform transposition of *all* grounds for transfer contained in Article 26 in *all* Member States. More than 25% of the data controllers who responded to the on-line consultation supported more flexibility for intra-group transfers where there is a controller in the Community and so did the majority of business associations. The Ministry of the Interior of the Land Baden-Württemberg made the point that companies that have binding rules of conduct should be in a position to determine themselves whether or not these rules constitute sufficient guarantees in case of transfer to another part of that company, in other words, a single authorisation to transfer personal data from the Community should be enough.

The Commission considers the general approach set out in Articles 25 and 26 necessary to prevent circumvention of the system. It would like to recall in that respect that Article 26 of the Directive, if implemented correctly and in all the Member States, offers companies a flexible system for the transfer of personal data to countries that are not considered as providing for adequate protection. Further to that, the Commission wishes to recall that it has undertaken considerable efforts to contribute to a secure and consistent framework for personal data transfers to third countries. Indeed, this issue has been one of the Commission's priorities in the field of data protection. Apart from the adequacy findings on the Swiss, Hungarian and, partly, the Canadian, laws and the US system of the Safe Harbor, the Commission has approved two decisions on standard contractual clauses under Article 26 (4) that provide additional means for a transfer of personal data to third countries. The initiatives promoted at the level of the Article 29 Working Party on codes of conduct for international transfers and the procedure of co-ordination presently under consideration by the national supervisory authorities constitute an important step in the right direction. The Commission considers, however, essential to carry out further work to facilitate transfers.

As regards **codes of conduct**, for the purpose of the Internal Market the adoption of Community codes is of course more important than codes at national level, although such codes may constitute a first step towards the development of Community codes on a particular issue.

Contributors were of the view that an improved/widened and streamlined procedure for the adoption of codes of conduct should be envisaged[78], with national codes of conducts

---

[76] See, for instance paper by BITKOM (Federal Association Information Economy, Telecommunications and New Media, Germany).

[77] See papers from C&W (Cable&Wireless), EPOF (European Privacy Officers Forum), or GDD (Association for Data Protection, Germany).

[78] The papers from AESC (Association of Executive Search Consultants Europe), Loyalty Partner and

benefiting from the principle of mutual recognition. Submissions also pointed out that the legal framework should leave sufficient scope to businesses to draw up their codes of conduct. Contributors stated that the ideal data protection "regulatory" system should define clearly the rules for compliance, the redress method, applicable laws, supervision, and ensure a consistency across all EU Member States and adequate countries. It should at the same time be fast and flexible enough to cope with different business, industry, country, and culture in constant evolution. Industry often argued that such constraints are difficult to solve with formal regulations, which would have to be carefully defined and would have to go through a complex and lengthy legislative process. Instead, self-regulation, added to an overall adequate regulation, would allow the necessary flexibility and timely adaptation. It is remarkable to note that, contrary to the positive general view of self-regulatory mechanisms, industry is bringing forward very few initiatives indeed in practice.

The Commission shares the views that self-regulatory mechanisms are a useful means to clarify and specify the law for particular sectors. It strongly encourages industry to take a more pro-active approach in the development of such codes.

As regards the monitoring of the application of transposition laws carried out by the **supervisory authorities**, an impact on the Internal Market might arise if the level of compliance with the legislation is very divergent in different Member States. Indeed, the level of awareness among controllers and data subjects and compliance appears to be rather low, although there are differences in this respect in different Member States. As regards the position of the authorities, the Commission notes with satisfaction that some Member States have undertaken efforts to further enhance the authorities' independence. It strongly encourages Member States to continue this effort.

Overall, it is the Commission's opinion that many of the problems described above have been created by incorrect transposition of the Directive rather than the Directive itself. However it is clear that certain provisions have suffered from definitional ambiguity and divergent interpretation, such as for instance parts of the applicable law provision in Article 4 (1)(c) or the interpretation of the notions 'personal data' or 'consent', and it is the Commission's intention to address these issues with the assistance of the Article 29 Working Party and through Interpretative Communications if necessary.

CBI (Confederation of British Industry) supported this.

Part 3: The application of the Directive to sound and image data

I. Introduction

Article 33 of the Directive states that the Commission 'shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons…taking account of developments in information technology and in the light of the state of progress in the information society'.

This part thus consists first of a brief description of technological developments and second of an analysis of how the Directive is applied to sound and image data in Member States, in the light of these technological developments. This analysis is limited to Directive 95/46, as indicated in the mandate of Article 33, and does therefore not examine the possible application of other directives, such as for instance the recently adopted Directive EC 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector which will enter into force in November 2003.

Given that only few Member States' data protection laws contain specific provisions on sound and image data, data protection authorities' guidance is of particular importance in this context.

This analysis is not meant to be exhaustive. Rather it looks at examples of the application of the Directive to sound and image data with a view to finding out whether these data raise specific issues in the application due to their particular nature.

II. Analysis

1. Technological developments

Recent years have seen an explosion in new technologies offering new means of processing sound and image data. The following technological features already exist and are among those that can be identified as having an impact on the processing of sound and image data and raise important issues in the application of data protection legislation[79]. Such are CCTV/video surveillance, especially in connection with face recognition; digitisation of images; 'reality-based' TV programmes; cameras in the workplace[80]; web-cams, i.e. distribution or diffusion of sounds and images over the web, e.g. in childcare centres; sharing of photos in the internet; recording of telephone calls,

---

[79] This list is by no way meant to be exhaustive. For an early, but very comprehensive study on various technologies processing sound and image data see CNIL, *Voix, image et protection des données personnelles,* (Paris 1996).

[80] See in more detail the Report of Giovanni Buttarelli, *Protection of personal data with regard to surveillance,* (2000), and *Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance,* Council of Europe (2000).

digital audio files; car licence plate identification ; and biometric systems[81], such as for instance digital fingerprints, face recognition, iris scanning or speaker verification. It appears that these technologies do not fundamentally differ from technologies used for processing other data in that they operate by digitalisation of data.

One may attempt to divide these features into two separate categories, one for sound and another for image technologies. However, some can fall into both categories, such as the first three ones listed above. It will thus not contribute much to the survey or analysis in the following to undertake this kind of categorisation.

In data protection authorities' practice, there appears to be a very strong focus on video surveillance and on biometrics, an issue that saw a particular increase in the last two years. The analysis will thus mostly deal with the application of data protection legislation in Member States to these features.

As regards future technological developments, such are of course difficult to predict. What appears to be certain, however, is that future systems will further facilitate the processing of personal data and thus increase the amount of data processed due to enhanced computer processing capacities. It also appears that such future technologies will seamlessly merge the processing of sound and image data into the processing of other data. Indeed, more and more data will be captured in 'bites'. Examples that already exist include vocal recognition systems that operate on the basis of voices that are reduced to digital form on a template, or a picture of an iris in electronic form. Thus, sound and image data will not stand out from other types of data.

2. Member States' provisions and guidance on sound and image data

Despite the rather cautious wording used in recital 14 of the Directive, according to which the Directive 'should be applicable' to processing involving sound and image data relating to natural persons, it is clear now that all Member States apply the Directive to such data.

Most Member States do however not specifically regulate the processing of sound and image data in their data protection laws and apply the general provisions to sound and image data instead. The notable exceptions are Luxembourg and Germany. The law in Luxembourg of 2 August 2002 explicitly states that the law applies to any processing of sound and image data, as long as these are capable of constituting personal data, and surveillance is defined as 'any activity which uses technology to detect, observe, copy or register movements, images, speech, writings, or the state of any object or person'. A further article lays down a list of criteria which make the processing of surveillance data lawful, such as for instance consent of the data subject or if surveillance is necessary for security or the prevention of accidents in places other than private residences. This article

---

[81] I.e. applications of biometric technologies that allow the automatic identification and/or authentication of a person by either physiological-based techniques or behaviour-based techniques. The system extracts from the biometric data user-specific features to translate these into a digital template form. See for more information: Registratiekammer, *At afce value: On biometrical identification and privacy*, (September 1999).

also stipulates that data subjects be informed of the processing by appropriate means and sets out conditions for further processing. The German data protection law of May 2001 now includes a specific provision on video surveillance, termed 'monitoring of publicly accessible areas with optic-electronic devices'. The law states that surveillance in such areas and with such devices is allowed only if it is necessary to fulfil public tasks, to exercise the right to determine who shall be allowed or denied access or to pursue rightful interests for precisely defined purposes, and if there are no indications that the data subject's legitimate interests prevail. It shall be discernible by appropriate means whenever an area is monitored and the controller's identity shall be provided. Data may only be processed, or used, if video surveillance is necessary for the pursued purpose and if there are no indications that the data subject's legitimate interests prevail. In addition, data may only be processed or used for another purpose if this is necessary to avert dangers to state security or public safety or to prosecute crimes. Where data are attributed to an identified person, the latter shall be informed about the processing or use. The data shall be deleted without delay if it is no longer needed for the pursued purpose or if the data subject's legitimate interests stand in the way of any further storage. This provision entails the data subject's claim to demand the erasure of personal data.

Denmark, Sweden and Portugal have special provisions on video surveillance in separate laws, such as the Act on Illicit TV-Surveillance (Denmark), the General Camera Surveillance Act and the Covert Camera Surveillance Act (Sweden) and a Regulation on video surveillance that sets up criteria that need to be met in order to obtain the necessary permission from the data protection authority before putting the system in place (Portugal).

In almost all the other Member States data protection authorities have issued general guidance. In response to the need, this guidance mostly deals with video surveillance. For instance, the Italian *Garante* has drafted the so-called *Decalogue* which lays down the main principles for carrying out lawful video surveillance. Detailed guidance also exists in the Netherlands, the UK, Finland, Belgium and Portugal. There are also numerous decisions by the data protection authorities that, again, focus on video surveillance, in general and for traffic management purposes in particular and, less, on biometrics These guidance and decisions are dealt with in more detail below. The only country where neither specific provisions in the law nor guidance by the data protection authority appear to exist is Austria.

3. Application of certain provisions of the Directive to sound and image data

Sound and image data might raise specific issues for the application of the Directive, given the particular nature of these data. This section examines how the Directive is applied in this respect in Member States. Given that only very few Member States have specific provisions on sound and image data, as described above, the general guidance and decisions by data protection authorities are of particular relevance. Where guidance relates to so-called third pillar issues, such as for instance public security measures taken by police, it is outside the scope of the Directive and thus not dealt with in this analysis.

a. Definition of personal data

The main issue in this respect is to see how the definition of personal data as 'any information relating to an identified or identifiable natural person' is applied to sound and image data. The guidance of data protection authorities deals with the application of this definition to images (photographs) on the one hand, and to biometric data on the other.

As regards images, the Danish and Swedish authorities for instance both distinguish between *portrait photographs* and *situation photographs* which are both covered by the definition of personal data once a person can be identified, ie recognised. According to guidance issued by the Finnish authority, personal data in the case of video surveillance is defined as information 'bound to a platform' that can be linked to an identifiable person. According to the French law of 1978, sound and image data constitute indirect nominal information (*informations indirectement nominatives*) whenever they allow to identify the person to whom they refer.

In the context of biometrics, according to the interpretation of the data protection law in Germany, the definition of personal data is a relative concept and ultimately depends on the information that the data processor holds on the data subject.[82] In the case where data consists of an individual's face there is a strong likelihood to identify the corresponding individual. A different situation arises according to this interpretation where data consists of nothing more than a fingerprint. The latter case is presented as an example where it would be doubtful whether personal data actually exist.[83] Hence, whenever it is generally not possible to match data to a certain person, e.g. by reference to additional knowledge, statistical procedures or external data, biometrical data would not constitute personal data.[84] In a study commissioned by the Dutch DPA, the authors argue that in the context of biometrical information 'the data involved will remain personal data in most, if not all stages of their processing[85]. A further study concludes that if information cannot be traced back to a person, or only with a disproportionate effort, such information shall not constitute personal data. For instance, a fingerprint might be anonymous when it is not possible to find the person from whom the fingerprints originate[86].

2. Definition of processing

As regards the notion of processing, most countries apply their legislation to the mere monitoring of data subjects without storage of any data. In the context of video surveillance one might refer to an *Avis* of the Belgian authority of January 2000 stating that processing in context of video surveillance takes place as soon as the device is being

---

82 A summary of this discussion is provided by Bäumler, et.al., *Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen*, (Unabängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2001), pp. 14ff.

83 See Ibid., p. 15.

84 Gundermann/Köhntopp, *Biometrie zwischen Bond und Big Brother: Technische Möglichkeiten und rechtliche Grenzen, in: Datenschutz und Datensicherheit*, 23/3 (1999), p. 147.

85 *At face value*, Registratiekamer, 1999, p. 35.

86 See: Grijpink, *Biometrics and Privacy, in: Computer Law and Security Report*, 17/3 (2001), p. 156.

used, regardless of possible storage. The Greek data protection authority's Directive on Closed Circuit Television Systems (September 2000) considers that processing of personal data is carried out by storage or transmission of personal data through fixed CCTV, operating on a regular, continuous or permanent basis and indoors or outdoors.[87] Mere recording without storage or further processing of images by CCTV does not exempt the data controller from the obligations under the DPA.

The UK Information Commissioner also adopted a wide interpretation in the CCTV Code of Practice 2000, stating that 'even the least sophisticated capturing and use of images falls within the definition of processing in the 1998 Act.' The latter includes simple recording and real-time transmission of images. Both the Danish and Swedish authorities also apply their legislation to cameras surveying an area without recording, as it implies processing of personal data using automatic means. In Sweden, manually collected personal data is covered by the Act, when it is to be used in a register. The Finnish ombudsman states in his guidance that the data protection law shall apply when personal data is processed, either using a 'registering video surveillance system' or collecting personal data through other types of video surveillance systems.

It is worth mentioning that in the discussion prior to the enactment of the implementation law in Sweden questions were raised about the concept of 'automated processing' and its scope. The processing of data on computers (in binary format), and the transmission in such a format, were clearly covered by Directive 95/46/EC. More uncertain however, was the extent to which non computerised formats should be covered by the term, for instance recording of sound and images in analogue formats (a negative, a tape or a video-cassette). The mere transmission of a person's appearance or voice to an analogue format, did, in the opinion of the *Datalagskommittéen*, the committee preparing the new law, not satisfy the term used in recital 15 of the Directive. However, it could still be argued that this was an automatic process, as the recordings are started and ended without a controller's direct influence (as in video-surveillance or telephone tap); and the computers or other electronic devices do the recording without direct human infiltration. The committee argued that the same uncertainty, *inter alia*, related to the use of mechanical clocks and cash registers (whose purpose is to register a worker's arrival at work). It finally decided to support a wide reaching definition in Swedish law, aimed at covering even partly automated processing.

The German provision on video surveillance appears to apply to mere monitoring also, given that there is a specific definition in the law on the mere collection of data. Some commentaries on the law, however, consider that monitoring is not enough to satisfy the criteria of that provision which according to them necessarily requires additional storage or evaluation.[88]

In France, if an image is digitised (*numerisé*), the whole system constitutes an automatic processing of nominal information and falls under the scope of the data protection law of 1978. French law draws a sharp distinction between video surveillance within the scope of Law No 95-73 relating to security and, on the other hand, the general data protection

---

87 See Directive on Closed Circuit Television Systems, 1122/26-9-2000, p. 1ff.

88 See Gola/Schomerus, *BDSG Bundesdatenschutzgesetz, Kommentar*, (2002), § 6b RN 10.

law of 1978. Recordings obtained through video surveillance are not considered as 'nominal information' (*informations nominatifs*)[89] in the sense of the data protection law 1978 unless they are assembled in a nominal file (*fichier nominatif*). As a consequence, mere recording falls under the scope of the Law No 95-73 relating to security. In contrast, recording for the purpose of establishing a nominal file renders the law of 1995 inapplicable and the law of 1978 exclusively applies.

Processing in the case of biometrics appears not to raise this issue since personal data are generally stored or forwarded by the system.

4. *Proportionality principle*

As far as the processing of sound and image data is concerned, the national practice strongly focuses on the concepts of 'necessity' and 'proportionality'. Many of the technological devices involved in the processing of sound and image data, such as digital fingerprints and CCTV, are likely to impinge on individual's privacy rights and are therefore subject to strict scrutiny by national data protection authorities.

Video surveillance in general

Concerning video surveillance, the data controller has to demonstrate that the technologies involved are the least-restrictive and constitute an adequate means to achieve a legitimate purpose. According to the guidance issued by several authorities, these principles entail, among others, the obligation to verify that there are no less-restrictive alternatives to video surveillance and the duty to record only images which are truly necessary, i.e. to monitor only those areas that are intended to be covered for a specific purpose.[90]

According to an *Avis* of the Belgian authority, the proportionality principle would restrict the use of surveillance to areas which are particularly dangerous, and the principle should be applied more strictly in areas which are not generally accessible to the public. In an interpretative directive the Greek authority states that generally, the recording and processing of personal data through CCTV on a regular, continuous or permanent basis is prohibited. Yet in exceptional circumstances, such as protection of individuals or goods and the regulation of traffic, it is considered to be lawful without prior consent. Criteria for lawful processing are, first, a 'necessity test' (i.e. least restrictive means) and, second, a 'proportionality test' (controller's interest vs. those of the individual). The fact that data shall not be excessive means that no more information than necessary is to be collected. Cameras in open spaces shall also not overlook entrances or the interior of private residences.

---

89 Which means "personal data" in the terminology of the French law. See the definition in Art. 4, Law No. 78-17, which refers to direct or indirect identification of individuals.

90 See, for instance, the Greek Directive on videosurveillance, the UK CCTV Code of practice, the Italian "Decalogue" on videosurveillance and the various decisions by national data protection authorities. See also the Working Document adopted by the Working Party 29 on 25 November 2002, on the *Processing of Personal Data by means of Video Surveillance,* p. 17 ff.

It might be useful to elaborate on some concrete cases in order to see the application of these principles in practice.

In Sweden in two cases[91] courts allowed camera surveillance in taxis under narrowly defined circumstances. The processing of personal data meant that pictures of the guests were taken just at the moment when they entered and left the taxi. The County Administration stated that a digital camera could take a maximum of five photographs in rapid succession (two seconds after the door was opened, with an interval of one second each). Sound recordings were prohibited, as well as any manual control over the camera by the driver. The aim of video surveillance in taxis shall solely be to ease police investigation when a crime is committed and to render the suspect's identification possible from the photographs in the taxi.

The French authority, the CNIL, decided on the transmission of images of a municipal crèche on the internet. The purpose of this system was to inform parents about the activities of their children during their time in the crèche. Only parents and some staff would have access to the web-site. The question which was raised by the CNIL was whether the measure was proportionate to its aims. The main principles of the system were the following: transmission of images only for a limited time and after information on the ongoing filming, secure transmission of images, no storage of images, (express) written authorisation by parents and staff. Allowing the cyber-crèche, the CNIL further requested express authorisation by staff members and parents as well as information on the recipients of images.

In Portugal, the authority dealt with a case of video surveillance[92]. The case referred to a company that had installed a system of video surveillance inside its lifts and had neither registered with the authority nor sought permission from the users of the building. The camera was installed in order to detect perpetrators of vandalism. Once the culprit being identified, the video was shown in a meeting with the directors of the company and the culprit. The latter subsequently filed a complaint with the authority, challenging the legality of the video surveillance system. The subsequent decision stated that unless the processing of data had been registered and permission requested prior to recording, the data had been illegally obtained. As a consequence it had to be destroyed. In addition, fines were imposed at the minimum amount required by the law.

Concerning the use of web-cams to capture images of a beach and meteorological information, the Italian data protection authority held that no filming in low resolution or zooming in on individuals should be possible, because the principle of proportionality also required that cameras should not be installed too close.[93]

The opposite approach appears to have been taken in the UK CCTV code of practice. The code states that the quality of images must be as clear as possible, in order to make the surveillance *effective* for the purpose for which it is intended. This might necessitate infrared equipment in poorly lit areas, according to the code.

---

91 Kammarrättens mål nr. 1166-2002 and Kammarrättens mål nr. 956-2002.

92 Deliberation No. 30/2000.

93 Decision "Videosorveglianza – Web-cam su spiagge" of 14 June 2001. See further Decision "Città di Mantova – Progetto di tele-sorveglianza" of 7 March 2000.

Video surveillance for traffic management purposes

There are some decisions on surveillance for the particular purpose of traffic management.

In France, in a case on number plate recognition, devices should have been installed on motorways. The purpose was to register information on cars that used these motorways. The following data would be registered and stored for one month: number plate, image of the car (but without filming the car's passengers), some traffic data such as speed, and distance, and date and hour of passing. Drivers would be informed through signs, which would also provide a phone number for further inquiries on the system. The purpose of the system was to improve both the quality of services provided by the company and security. The CNIL held that such a system would restrain constitutional rights and aim at diminishing the right to private life, especially since people would not be able to move anonymously anymore. In addition, the company could control whether drivers would commit infringements of the '*Code de la route*' – a task exclusively conferred on police forces and the *gendarmerie*. The CNIL thus prohibited this system of video surveillance.

According to a directive issued by the Greek data protection authority, in cases of video surveillance for traffic management purposes 'the recognition of faces or vehicles shall be possible only whenever necessary to achieve the purpose each time pursued. For example, if the aim of image recording is to control the traffic flow and not to detect traffic offences, the cameras shall be placed in such locations so that they do not allow face or vehicle recognition'.

In Portugal, as regards the regulation of data related to the surveillance of traffic and motor vehicles, a number of provisions are relevant: Law-Decree No. 54/75, Decree No. 55/75, Law-Decrees No. 242/82, 217/83, and 54/85. These rules extend the possibility to legally transmit such data to different administrative authorities as long as the data contain no more than the vehicle's licence (number plate) and a description of the vehicle. The Portuguese data protection authority stated that the owner's name, address, or other data may not be stored.

Biometrics for the purpose of access control

As regards biometrics for the purpose of access control, national data protection authorities have developed detailed guidance. It restricts the use of such devices to those cases in which the devices are proportionate to the aims sought (i.e. mainly security-related). The Greek data protection authority stated in this context that it is not possible to substitute lawful processing or the principles of purpose and necessity with the consent of the data subject. Due to the proportionality standard (which involves a balance of interests), the processing of digital fingerprints is allowed only in exceptional circumstances (fingerprints could be misused for other purposes than originally intended and make individuals traceable)

The CNIL issued some decisions on the use of digital fingerprints as a means of controlling access to facilities. The *Avis* 'Banque de France' (1997) dealt with access control for high security zones by means of digital fingerprints and codes. The data would only be stored as long as the person worked for Banque de France and information

relating to individual access would only be stored for three months. Generally, the data was intended to only be used by personnel responsible for security.

Another *Avis* (2000) dealt with the request made by a Préfecture that wanted to use digital fingerprints (in connection with a personal badge) to control working hours of staff. The digital fingerprint would prevent fraudulent use of badges by colleagues. The registration of digital fingerprints would allow identification of persons in various circumstances and was therefore said to be potentially capable of being used for other purposes than for those for which it was initially designed. The CNIL had to decide whether a database of personal data, which allows the identification of persons, was proportionate to the aims sought.[94] According to the CNIL, the creation of a database containing digital fingerprints was not proportionate to the aim of preventing fraudulent use of badges by other members of the staff.

A further *Avis* (2000) related to a request made by the Ministry of Education that wanted to set up a system of access control to buildings for the educational staff. The intention was to use digital fingerprints. The aim was to guarantee secure access to those buildings (without the need to distribute badges among the personnel) and not to control working hours (time and data of access would not be registered). According to the general statement of the CNIL: *'Le recours à la biométrie associée aux nouvelles technologies peut être de nature à apporter une réponse adaptée à certaines situations dans lesquelles l'authentification ou l'identification des personnes doit être parfaitement assurée.'* The CNIL repeated a former statement saying that a database of digital fingerprints makes persons traceable and may be used for other purposes than those for which it was originally intended. Under these circumstances the CNIL required the biometrical technologies to be adapted and proportionate to the aims sought. Generally, the aim of an access control system for buildings, which mainly intends to facilitate access for staff, cannot justify the establishment of a database of digital fingerprints. Only the limitation of such a system to sensitive areas (with confidential material) may be justified. When such a system is in place, it needs to consist of three different sets of data: 1) personal information, 2) access rights, 3) the digital fingerprint (in encrypted format).

Another *Avis* (2001) was issued upon a request made by the Louvre. The Museum wanted to set up a biometrical access control, which would identify the contours of the hand. The aim was to control working hours of staff and guarantee security of access. It was intended that the data (on individuals) would only be stored as long as the individual would be employed by the Louvre. Access data (date, time) would be stored for one year. The CNIL concluded that the contours of the hand do not constitute data which is likely to be used for other purposes than those for which it was initially set up. Contours of the hand do not leave traces (e.g. like digital fingerprints) which prevents the data from being used for other purposes. The *Avis* 'URSSAF' (2002) dealt with the processing of digital fingerprints used as access control to buildings in Corsica. The CNIL stated that digital fingerprints could potentially be used for other purposes than those for which they were initially constituted, and therefore other means of biometric access control were preferable. The system in Corsica would only concern a few people and give access to a single floor in a building which is guarded by other means. The system would not be able to prevent terrorist attacks to which the Radio station has been subject in the past. Since

---

[94] General guidance on badges for work purposes: information on entry/exit hours: 3 months storage (or otherwise necessary).

this measure would not prevent access to buildings by unauthorized persons, the CNIL rendered a negative avis.

In a recent *Avis* (2002) the CNIL dealt with biometric access control (contour of the hand) that should be used in school restaurant. The CNIL allowed this technique since it would not leave 'traces' and could not be misused for any other than the original purpose. In a previous decision the CNIL had held that access control for a school restaurant based on digital fingerprints would pose too many dangers for misuse and, consequently, was excessive.

In Greece, the data protection authority issued a decision relating to biometric data in identity cards for Greek citizens. The decision was, amongst others, based on the Law 2472 and the Directive 95/46/EC. In its decision the Data Protection Authority held that '[a]ny processing of personal data which exceeds the pursued purpose or which is neither appropriate nor necessary for the achievement of such purpose is considered to be unlawful.'[95] The purpose of identity cards is to verify the identification of the data subject. On these premises, the Data Protection Authority held that the processing of a number of personal data on identity cards would exceed the said purpose: Most relevant for the scope of this study are fingerprints. They were held not to be necessary for the purpose of verifying identity (which is evident from the photo) and, in addition, were held to offend human dignity.[96] The decision further stated that the processing remains unlawful even in situations where the data subject has given his consent. It is therefore not possible to derogate from lawful processing or the principles of purpose and necessity through the consent of the data subject.

A different decision focused on the use of fingerprints in the workplace.[97] The Greek authority reiterated that processing of personal data shall be based on the principle of proportionality which means that more moderate means, achieving the same purpose, should be used. Generally, fingerprints are taken by law enforcement agencies on the basis of legislative provisions. The Data Protection Authority ruled that taking fingerprints to monitor the presence of workers would not be proportionate and carry less weight than the individual's right to privacy. Only in exceptional circumstances (such as access to confidential files or high-security areas, safety requirements, etc), might taking of fingerprints at the workplace be acceptable. The Data Protection Authority further stated that taking fingerprints is unlawful insofar as it exceeds the purpose, and, as a consequence, it could not be justified by individual consent of the data subject.

In Italy, concerning the use of biometric devices, the *Garante* clarified the lawfulness of the use of digital fingerprints by banking institutions.[98] Encrypted fingerprint recognition systems are only allowed if the use of such systems relates to particular risks which are

---

95 Decision 510/17/15-05-2000, p. 4.

96 Similar arguments were used in relation to the full name of the spouse, the profession, residence and religion.

97 The same principle was confirmed in the Data Protections Authority's Directive 115/2001 concerning worker's files.

98 See "Rilevazioni biometriche in banca" (28 September 2001). See also the Decision of 11 December 2000, where the Data Protection Authority held that the use of fingerprints at the entrance of a bank was disproportionate since other less privacy-intrusive access control systems could be used.

being faced by the bank, personal data, originating from the fingerprint recognition system, is not filed and collected in a database, the access by means of fingerprint recognition system is voluntary, consensual and not the only way to enter a bank, the data is protected by an encryption system, data may only be decrypted by certain public authorities for the purpose of investigating criminal offences, encrypted data is deleted after one week, clear information is provided to the customers, and no face-recognition and indexation system is in place. (????)

5. ***Obtaining consent***

According to the definition of the Directive, consent means any freely given specific and informed indication of the data subject's wishes. There seem to be few cases in practice where this issue is at stake. A Danish case demonstrates that the requirement of consent, here concerning the transmission of video surveillance, is not be satisfied by the mere fact that an individual passes by signs which indicate the transmission of images. Consent should be in writing and customers be informed about all aspects of the processing and the impact of their consent.[99]

As regards consent as a criterion for processing, the Danish authority recently issued guidance on the processing of pictures in the internet. As mentioned above, the authority generally distinguishes between situation photographs and portrait photographs. As a general guideline, situation photographs could often be processed without consent. For instance, 'harmless' photographs could be processed without consent- such as a photograph showing children playing in a schoolyard. A photograph showing guests at a night-club would however need consent. Consent would almost always be necessary for processing of portrait photographs. A balance of interest must be undertaken in each individual case.[100]

6. Storage period

Personal data may in principle not be stored for longer than is necessary for its purpose (cf. Art. 6 (1) e Directive 95/46/EC). The guidance provided by the *Garante* on video surveillance states that the storage period shall be defined in advance and after that date has expired the data shall only be kept for certain specific purposes. In Finland, according to a recommendation issued by the ombudsman, the controller shall have a look at the material that was gathered within three days and then decide whether further storing was necessary.

Data protection authorities have provided guidance on specific time limits for different types of personal data. For instance, Belgium: images recorded in public places (one day); Denmark: general surveillance data, e.g. in supermarkets (30 days); France: surveillance data of public places (one month), processing of information concerning number plates on cars by customs officials (four or, exceptionally, 24 hours), no storage

---

[99] See Danish Data Protection Authority, J.nr. 2002-631-0086.

[100] Datatilsynet: *Offentliggjørelse af billeder på internet*, (26 September 2002).

of images in the 'cyber-crèche', biometric access data up to three months or one year; Greece: CCTV data (15 days, prolongation possible in exceptional cases and upon permission of the data protection authority); Italy: access control (one week); Portugal: CCTV data (30 days); Spain: CCTV data (30 days); Sweden: CCTV data (30 days); United Kingdom: CCTV data in pubs (7 days), CCTV data in public places (31 days), cash machines (three months).

7. *Sensitive data*

There are a number of decisions by the data protection authorities on whether certain image data should be considered sensitive personal data and thus fall under the particular protection foreseen by the Directive.

The Belgian Data Protection Authority held for instance that information on ethnic origin or health should not necessarily be treated as sensitive data if the information resulted from surveillance for a different purpose. However, if the purpose was to systematically record and acquire information according to the criteria determining sensitive data, processing of sensitive data would occur[101]. The Guidelines of the Dutch Ministry of Justice state that photographs on badges could reveal the employee's race and should therefore be treated as sensitive data. The discussion prior to the implementation of Directive 95/46 in Swedish law touched upon the question whether pictures containing information about race or health status (illness or even healthiness) would constitute sensitive data. The Committee preparing the new law stated that photographs involving persons in 'normal' situations do not aim at revealing sensitive data.[102]. A general exemption for 'harmless data' has subsequently been accepted by the Swedish data protection authority, for instance where data could arguably be classified as sensitive, they should still be possible to process, if they were clearly not harmful.

In a similar direction, the Belgian authority stated that processing images, which could relate to sensitive data, is not automatically prohibited, unless the data would be used to acquire systematic information on the persons concerned.[103]

In Greece, the processing of sensitive data, e.g. obtained through video surveillance in hospitals or insurance fund premises, is subject to prior authorization by the data protection authority. The authority ruled on the use of information on the sexual life of a famous Greek entertainer and fashion designer to create a file, containing sensitive personal data. The 'possession, recording in a file and television use of these data', which included pictures and videos, was ultimately unlawful and disproportionate for particular reasons[104].

---

[101] See Avis of 13 December 1999.

[102] See *Datalagskommittéen: Integritet - Offentlighet - Informasjonsteknik*, SOU 1997:39, page 371

[103] In the words of the Commission: "La constatation occasionnelle de la presence de ces données sensibles ne constitue pas un traitement au sens de l'article 6."

[104] Decision 100/31-01-2000.

Sensitive biometric data

As regards biometric data, it might be possible to classify templates capturing or measuring human characteristics as sensitive data; examples are facial images showing skin colour or illnesses.[105]

An opinion[106] of the Dutch data protection authority clarifies several issues in relation to the use of biometric data. The biometric system in question was used as a tool for access control of visitors, e.g. for sports events. It was based, inter alia, on face recognition. The Dutch authority stated that the processing of images of faces would constitute sensitive data insofar as the race of a person could be determined (which would not be the case for fingerprints). Sensitive data concerning one's race may only be processed with a view to identifying data subjects and only where this is essential for that purpose or where the data subject has given his explicit consent. The Data Protection Authority accepted that the processing of biometric data was necessary for this kind of access control, especially to prevent certain people from entering a stadium.

The Greek data protection authority issued a decision on DNA analysis for the purpose of criminal investigation and penal prosecution (401/15-02-2001). Relevant for the scope of this study is the characterization of genetic data as 'sensitive data' since it not only reveals individual health, but also racial or ethnic descent. In addition, the authority stated that genetic analysis should be restricted to 'extremely serious crimes' and no data should be collected for mere preventive purposes.

Processing for artistic expression

Recital 17 of the Directive states that as far as the processing of sound and image data is carried out for purposes, i. al., of artistic expression, the principles of the Directive are to apply in a restricted manner according to the provision laid down in Article 9 of the Directive.

There is one example of a concrete application. In a Danish case[107], the data protection authority dealt with a TV-project, where the transmission of 'live documentaries' from existing surveillance-cameras at a shopping mall was intended to be transmitted on local-TV and on big screens in the mall and a housing area close by. The surveillance as such was not covered by the Act on Illicit TV-Surveillance, as the Act does not ban surveillance in shopping malls. The authority stated that surveillance activity was processing of personal data, emphasising that people filmed could be identified. The project was an artistic expression called 'public access', aimed at implicating the citizens in the production. As a documentary it also had a journalistic idiom. The authority approved it as such and hence Danish data protection legislation was not longer entirely

---

[105] For further information see: Dutch Data Protection Authority, *At face value – on biometrical identification and privacy* (1999), p. 16. See further the policy discussion in the Report prepared by Spiros Simitis, *Revising Sensitive Data*, Council of Europe (1999).

[106] **Biometrisch toegangscontrolesysteem (discopas), (March 2001).**

[107] J.nr. 2002-321-0155.

applicable.[108] Therefore did not derive from the Agency's competence to further comment on rules for the data processing.

8. Information to data subjects

Data subjects must be informed about the processing of sound and image data in line with Articles 10 and 11 Directive 95/46/EC. In the case of video surveillance, including the use of web-cams, this incorporates the duty to provide a notice, according to the guidance issued by several authorities. Such a notice shall clearly and effectively specify the purpose of surveillance to the data subject from whom the data is collected.[109] Such a notice could be set up in a block of flats, a stadium, in the streets, on motorways or in shops. In Sweden, in case there is additional sound recording, this would require a further explicit statement on sound recording.[110]

As regards the content of the notices, a report issued by the Danish authority on surveillance[111] specified that regarding video-surveillance, clear signs informing about the surveillance were found adequate in relation to the customers. It was found that further information to the data subject proved impossible or involved disproportionate effort. This means that the Danish authority applies Article 11(2) of the Directive- 'information proves impossible or would involve a disproportionate effort'- to this situation, and thus considers these kind of data as information that has not been obtained from the data subject. However in relation to the employees, the authority stated that precise information and express consent were required. The employees were entitled to information on a number of issues including the following: what was the aim of the surveillance (this could for instance be crime prevention, explicitly stating whether this also concerned the employees); where was the surveillance going on?; how long the data were kept; when the data could be assessed; and finally, whether the data could be given to the police and under which circumstances?

9. Access

As regards the right of access, the usually short retention period of images might narrow the scope of application of this right, as the Working Party 29 pointed out recently[112]. Further to that, when a data subject requests to exercise his access rights, this may collide with rights of third parties whose images would have to be disclosed as well.

---

[108] Cf. the exemption for such in Art. 2 (10) according to which only articles 41, 42 and 69 of the Act apply.

[109] See e.g. Italian Data Protection Authority, *Decalogue*, (2000), the decisions of the CNIL on videosurveillance, Portuguese Regulation DL No. 231/98 or guidance by the Finnish ombudsman.

[110] See Art. 3 Swedish General Camera Surveillance Act.

[111] J.nr. 2001-211-0027.

[112] Working Document on the Processing of Personal Data by means of Video Surveillance, p 17.

The UK Information Commissioner adopted an approach taking into account the varying degrees of duty of confidence owed to a third party in the CCTV code of practice. According to this interpretation, the duty of confidence mainly depends on where images have been recorded; streets would give rise to less of an expectation of confidence than would be the case indoors or in the private sphere.

Further to that, image data recorded for surveillance purposes are not structured in a way that allows easy access to these images. This appears to be an issue where the literal application of the Directive might be problematic. However, according to the Working Party 'this right is to be safeguarded especially if a detailed request is made such as to allow the relevant images to be easily retrieved[113].

III. Conclusion

From this review of the practice in Member States there are no indications that the Directive cannot be applied as such to sound and image data due to a special nature of these data. Indeed, data protection authorities have been able to deal with issues relating to sound and image data on the basis of the existing Directive. As regards the issue of the data subject's access, especially to data captured through video surveillance that are stored for only a short period and are not easily accessible, the Working Party 29 recently noted that 'any limitations grounded on the efforts to be made for retrieving the images, where such efforts are found to be clearly disproportionate on account of the short retention period of the images, should be laid down exclusively by primary legislation (see Article 13(1) of the Directive) with due regard for the data subject's right to defence in respect of specific events that may have occurred in the period considered'[114].

For the moment, there is no evidence that one particular technology poses problems in terms of application of the Directive. On the contrary, it appears that sound and image data and other types of data will more and more converge in the sense that they are all processed by digital means. Thus, sound and image data will less and less be of a particular nature. The Commission will continue monitoring technological developments.

What the analysis did prove, however, was that Member States interpret certain provisions of the Directive divergently, as for instance regarding sensitive data. This finding is confirmed by the analysis of the implementation of the Directive in Member States. Such divergent interpretation is, however, not due to the particular nature of sound and image data, but the result of differing concepts used by Member States when assessing whether personal data constitute sensitive data.

---

[113] Ibid., p. 17.

[114] See Working Document on the Processing of Personal Data by means of Video Surveillance, p. 21.