EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE
(Study Contract ETD/2001/B5-3001/A/49)

comparative summary of national laws

by

Douwe Korff
(consultant to the European Commission)

Human Rights Centre
University of Essex
Colchester (UK)

Cambridge (UK) September 2002

About this report

This paper provides a *comparative summary* of the national data protection laws in the Member States of the European Union. In accordance with the contract under which this work was done, its aim is to clarify whether there are differences (or divergencies) in the way in which these laws are applied; and to enable the Commission to assess whether such divergencies cause obstacles to the Internal Market.

In twelve Member States, the laws are new or amended laws, adopted or amended with a view to implementing Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (hereafter referred to as "the Directive"). However, when the work on this summary started, in the autumn of 2001, three Member States - France, Ireland and Luxembourg - had not yet adopted legislation to implement the Directive, and the Commission had taken enforcement proceedings against them. By the time the summary was being finalised, in September 2002, Luxembourg had adopted a new law, which is to come into force in December of this year; Ireland has passed a statutory instrument bringing some important aspects of the law into line with the Directive, while a Bill further amending the data protection law had been passed by the Upper House of the Irish Parliament (the *Seanad*) and was pending before the Lower House (the *Dail*); and a draft law amending the French data protection law had had its first reading in the National Assembly.

In this summary, I refer to the new Luxembourg law (the Law of 2 August 2002), although of course there is as yet no practice under that law; to the new law in Ireland (by which I mean the Data Protection Act 1988, as it will be if the Data Protection (Amendment) Bill 2002 is adopted in its current form); and to the new law in France (by which I mean Law No. 78-17 of 6 January 1978, as it will be if the *projet de loi* amending that law is adopted in its current form). For the sake of brevity, I may, from time to time, refer to these laws as the "new law" or the "new (amended) law" in the country concerned. If I refer to the current laws in these countries (in particular in respect of matters which will remain unaffected by the proposed amendments), I may call them "the current law" or "the current (pre-implementation) law".

I should stress that the current (pre-implementation) laws in France and Ireland in many - indeed, most - respects already conform to the requirements of the Directive - if only because they conform to the Council of Europe Convention on data protection (Convention No. 108), which also provided the starting point for the Directive. Certain matters - in particular, the question of "applicable

law" and transborder data flows - require substantial changes to these laws; otherwise, the laws need to be amended in specific contexts only. To the (large) extent to which the laws already conform to the Directive, I have therefore been able to refer to practice under these laws to illustrate certain matters addressed in the Directive - just as I have been able to refer to practice in the other Member States under their previous laws where such practice clarified relevant issues.

The purpose of this summary is not to provide an encyclopaedic description of all the rules in all the data protection laws and subsidiary rules and regulations, case-law and related legal rules, covering matters covered by the Directive. Rather, its aims is to describe in a ***comparative and analytical way*** the laws in the Member States, to support the aim of the study, as set out above. Extensive reference is nevertheless made to case-law and subsidiary rules and interpretations of the laws in theory and practice.

Each of the sections in this summary starts with a short **introduction** to the topic, a **comparative summary of the findings**, and a brief statement of the **matters to be further clarified or addressed**. Some sections, which deal only with a single issue, are confined to this. In most sections, however, this is followed by more detailed comparative summaries (in smaller print) of the findings concerning specific sub-issues (as listed in the Contents).

Some of the sections go beyond a description or summary of the situation in the Member States to touch on more general issues, in anticipation of the Conclusions and Recommendations. Thus, section 1 does not only discuss the constitutional status of data protection in the Member States, but also the constitutional position of data protection in the European Community and – Union. Section 3 covers not only the question of the substantive scope of the national laws, but also the status of the national laws in the relevant legal system as a whole. And section 15 deals not only with codes of conduct, but also with other sectoral rules and other measures to clarify or further determine the application of the laws in specific contexts (including technical standards).

Douwe Korff
Cambridge (UK)

C O N T E N T S :

(continued)

CONTENTS (continued):

(continued)

CONTENTS (continued):

- o – O – o -

1. constitutional status of data protection [Art. 1(1)]

introduction: the status of data protection in Community- and Union law

> "... the object of the national laws on the processing of personal data is **to protect fundamental rights and freedoms**, ***notably the right to privacy***, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law" (10th Preamble to the Directive)

> "In accordance with this Directive, Member States shall **protect the fundamental rights and freedoms of natural persons**, ***and in particular their right to privacy with respect to the processing of personal data***." (Art. 1(1) of the Directive – **object of the Directive**)

It is clear from Art. 1(1) of the Directive and from various preambles, including in particular the 10th Preamble, quoted above, that one of the main aims of the Directive is **the protection of the fundamental rights and freedoms**, and "in particular" the ***right to privacy***, of individuals ("natural person") with respect to the processing of data on such persons - even if this is only because without such protection the other (and perhaps primary) main aim of the Directive (free movement of data within the Community as a means towards the smooth operation of the internal market: Art. 1(2)) cannot be achieved. ***Data protection is human rights protection, and the Directive is therefore a human rights instrument.***

The fact that the Directive seeks to protect fundamental rights gives it a special status in Community law, because such rights - in particular, as set out in the substantive provisions of the European Convention on Human Rights - constitute "**general principles of Community law**", of ***overriding, constitutional importance within the legal order of the Community*** (and indeed the Union).[1] When the Directive was drafted, this was reflected in particular in Art. F.2 of the Treaty on European Union (which confirmed the case-law of the Court):

> "The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community Law."

[1] See: D Korff, *Human rights in the European Union*, Cambridge\Bilbao, 1994; B de Witte, *The Past and Future Role of the European Court of Justice in the Protection of Human Rights*, in: Ph. Alston (ed). The EU and Human Rights, Oxford\Florence, 1999, p. 859 ff.

The 10th Preamble to the Directive expressly recognises this **constitutional status** of data protection, with reference to the Convention and (again) "notably" to privacy which, it rightly says, "is recognised both in Art. 8 of [the Convention] and in the general principles of Community law".[2]

Since the coming into force of the Directive, the protection of fundamental rights in the Union has been further strengthened by the adoption of the EU Charter of Fundamental Rights of the European Union. The Charter confirms the rights already recognised in the Convention, including the right to respect for one's "private and family life, home and correspondence" (Art. 8 ECHR) - which it somewhat modernises by referring to "private and family life, home and *communications*" (Art. 7 of the Charter) - but the Charter also, for the first time, explicitly makes **data protection a fundamental right of its own**:

> Article 8
> ***Protection of personal data***
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

The Charter also (as further discussed below, at 10) confirms the **right to freedom of expression**, including the "***right to receive and impart information without interference by public authorities and regarless of frontiers***" (Art. 11 of the Charter, confirming the right guaranteed by Art. 10 ECHR, but with an added reference to respect for the freedom and pluralism of the media); and adds a further **right** (not contained in the Convention) **of access to public documents** (Art. 42 of the Charter).

The Directive, and the laws implementing the Directive, therefore operates, and operate, in a highly sensitive context, touching on fundamental, constitutional interests of the Union and the Member States - and their citizens.

---

[2] On the international-legal background to data protection, see my earlier study: D Korff, Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons (Study Contract ETD/97/B5-9500/78), European Commission, Brussels, 1999, Chapter 2: *the international legal framework for data protection*.

the status of data protection in the Member States

As already noted in another earlier study by me for the Commission,[3] ***the nature and status of data protection in the Member States varies***. Some countries (e.g. the Netherlands, Portugal, Spain) have specific data protection provisions in their **constitutions**, similar to Art. 8 of the Charter, which to some extent treat data protection as a ***sui generis right*** - although in their law or case-law they may also ***link*** it to other general or specific rights, such as the right to respect for privacy or private life (Portugal, Netherlands), or private and family life and honour (Spain) and\or to the general (proto-)right to respect for one's "personality" (Netherlands). In Austria, data protection is expressed (in the Law) in the form of a constitutional **right to secrecy** (or ***confidentiality***) **of personal data** - but also linked to the right to private life.

In other countries, data protection is directly ***derived*** from **general or specific constitutional principles**, without being explicitly mentioned in the Constitution or in constitutional provisions. Thus, in Germany - in which data protection is given a high constitutional status - the principle is nevertheless not explicitly mentioned in the Constitution but derived from the "***general right to [respect for one's] personality***" (*das allgemeine Persönlichkeitsrecht*) - although there are calls for a more explicit constitutional provision. In France, data protection is based on the (linked) constitutional requirements of respect for "***human identity***" and ***human rights***, ***private life*** and ***individual and public liberties***. Other countries link data protection to "***privacy***" or "***private life***" (Belgium, Luxembourg), "***private life and honour***" (Finland), "***privacy and personal identity***" (Italy), "***private life, human dignity and –value***" (Greece), or "***personal integrity***" (Sweden). In Ireland, too, data protection is considered to derive from the right to ***privacy*** - which itself has been recognised as an unenumerated (i.e. not expressly mentioned) constitutional right since 1937.

In several of these countries, the fact that data protection is constitutionally protected has **legislative implications** and **implications for the relationship between the data protection law and other laws**, as further discussed below, at 3.4.

In the United Kingdom, which does not have a written constitution, data protection was originally given no special status - but the country has now incorporated the European Convention on Human Rights in its domestic system, and given it enhanced (although not fully supra-statutory) status. This means

[3] D Korff, The feasibility of a seamless system of data protection rules for the European Union (Study Contract ETD/95/B5-3000/MI/169), European Commission, Brussels, 1998, section III.1: *the status of data protection in the national legal systems*.

that, to the extent that data protection can be said to derive from rights enshrined in the Convention - such as the right to "***private and family life***" - it now also enjoys **enhanced protection** in that country, with reference to those Convention rights. In many other Member States too, the link between data protection and the ECHR has implications, because of the special (indeed, sometimes supra-constitutional) status of the Convention in the relevant domestic system. This is again further discussed below, at 3.4.

In Denmark, there is no very firm constitutional basis for data protection; and no special status dervies from international human rights law either. There is no specific constitutional provision referring to it, and also no provision on privacy or private life. The European Convention on Human Rights is directly applicable in Denmark - but is not accorded supra-statutory (or otherwise enhanced) status.

Data protection in the Member States is thus **based on a range of somewhat different constitutional principles and rights**. Indeed, even if data protection is based on similar principles, this does not necessarily imply identical doctrines. Thus, in Germany, the Constitutional Court has developed a general principle of "***informational self-determination***" from the right to respect for one's personality. In France, the data protection authority (CNIL) has said that the general "***right to object***" to processing on "***legitimate grounds***" (which originated in France, as discussed below, at 9.2) is "the clearest and most tangible" expression of the concept of "informational self-determination" and the concept is therefore, in this sense, accepted there too. However, in the Netherlands, the Supreme Court has declined to adopt this view, even though it did relate data protection to the same "general personality right".

In other words, while there is **widespread agreement** in the Member States on the ***idea*** that data protection is a fundamental human rights matter, of constitutional importance, there also remains (as I already noted in another one of my earlier studies) a "***lack of clarity, of focus, over the very nature, aims and objects of data protection in the Member States***".[4]

This lack of agreement on the details of data protection is reflected in the different ways in which different Member States apply their laws to "legal persons" (see below, at 3), and in which they address the question of whether processing, in particular of sensitive data, on the basis of consent is always allowed (as discussed below, at 7). The ambiguity about data protection in

[4] D Korff, Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons (footnote 2, above), Chapter 3, *the legislative situation in the Member Stats (and three non-Member States)* and *Conclusions*.

constitutional\human rights terms also has a bearing on the question of how to reconcile data protection with other fundamental rights, such as freedom of expression and freedom of information (in the sense of a right of access to official documents), as discussed below, at 10.

matters to be further clarified or addressed

If the Directive is to be revised, the explicit recognition of its constitutional aim and -status should be retained and, if anything, further emphasised, in the light of new developments in Community- and Union law, and in particular in the light of the Charter. This should include an **express reference to the Charter** and the use of **terminology consistent with the Charter**. At the same time, the equally constitutional questions relating to the relationship between data protection and other fundamental rights (freedom of expression; freedom of information in the sense of access to official documents) should be further clarified.

As is clear from the differences between the laws in the Member States which derive from constitutional differences and ambiguities, alluded to above, these are not just "academic" matters. Member States are likely to adopt different positions on specific issues if they approach those issues from different constitutional perspectives. To that extent, **further clarification** about the exact aims and objects of data protection ***would help reduce divergencies*** - and thus obstacles to the Internal Market - most obviously with regard to the question of whether data protection can, or ought, to be extended to legal persons.

Another crucial constitutional matter, is that if there are rules in the Directive, or in the laws of the Member States implementing the Directive, which can lead to the erosion, avoidance or evasion of adequate data protection this would undermine the very foundations of the Directive. They would tempt Member States to re-impose restrictions on the free flow of data within the Community - indeed, in some countries the courts (or the Constitutional Court) would feel obliged to re-impose them. This would lead to serious constitutional problems at the national and European level, reminiscent of the problems reflected in the "*Solange*-" judgments of the German Constitutional Court (to which the human-rights-friendly case-law of the European Court and in particular its recognition of fundamental rights as "general principles of Community law" was a response).[5] The providing by the Directive, and through it by the laws of the Member States, of **adequate data protection, *without "loopholes"***, therefore remains ***a conditio sine qua non for the internal market***.

- o – O – o -

[5] See my paper on *Human rights in the European Union,* footnote 1 above.

2. definitions in and application of the laws [Art. 2]

introduction

Definitions in legal texts are crucial: ambiguities create uncertainties for some, loopholes for others, and invite costly and time-consuming legal disputes. **In a European context clarity in the definitions in the basic text and uniformity in their transposition into national law are essential.** Even minor changes in the wording of a definition can have significant effects on the application (or indeed applicability) of the legal rules in which the term is used.

The study examined the way in which the terms or concepts defined in Art. 2 of the Directive - **personal data** (and ***data subject*** and ***identifiable person***); **processing** (and ***disclosure***); **filing system**; **controller**; **processor**; **third party**; **recipient**; and **consent** - are defined and applied in the laws of the Member States. The study also noted various definitions in the laws of the Member States of ***additional concepts***, not defined in the Directive.

summary of findings

The study found that (leaving aside the issue of applying the laws to legal persons by including such persons in the definition of "data subject", discussed below, at 3) there are ***mostly* only minor variations** in the definitions in the laws of the Member States of the terms "***personal data***", "***processing***", "***filing system***", "***processor***", "***third party***", "***recipient***" and "***consent***" - but with some minor differences being capable of leading to divergencies in certain special cases, and with some laws adding certain matters which do clearly lead to differences; while there are **more significant differences** in the wording of the definitions of the concept of "***controller***" - but without this being likely to lead to serious differences in practice. Some laws, as a matter of legislative technique, leave out the **examples and clarifications** provided in the Directive. Conversely, further clarification - not provided either in the Directive or the national laws - would be useful in other respects, as further noted below, under the next heading.

As a result of seemingly minor additions or variations, some data will be regarded as "personal" in some countries, but not in others; some processing systems will be regarded as (sufficiently structured) "**filing systems**" to fall within the law in one country, but as insufficiently structured or easily-searchable - and thus outside the law - in another. Etcetera.

Furthermore, the exclusion of "***authorities which may receive data in the context of a particular inquiry***" from the concept of "**recipient**", contained in the Directive, is not followed in no less than seven Member States - which is clearly a reflection of some unease about this exclusion.

matters to be further clarified or addressed

In spite of **considerable convergence**, the definitions in the laws of the Member States still ***differ in detail***; and there are still certain matters which need to be ***clarified***. It would still be **highly recommendable** to bring the definitions ***fully in line*** with the Directive and thus with each other.

As far as matters of ambiguity are concerned, it must be made clear whether (or when) ***not-fully*** (or ***not-immediately***) ***identifiable data*** - such as ***encoded*** or ***pseudonymous data***, should always be regarded as "relating to an identifiable person", or whether this should only be the case if the person processing the data can link the data to such a person (typically, by means of a decoding "key" or number). In other words, it must be clarified whether the concept of "**personal data**" is ***relative***. Some Member States appear to feel that it should be regarded as such; others take the opposite view; while yet others are ambiguous in this respect. It should similarly be clarified when the use of ***geodemographical*** or ***statistical data*** etc. is such as to turn these data into "personal data". This question also has repercussions with regard to ***sound & image data*** and other data such as ***IP-addresses***. The reference in the Directive to controllers acting "***alone or jointly with others***" in determining the purposes and means of processing (which many Member States repeat in their laws without clarification) should also be clarified - preferably in such a way as to ensure that for each specific processing operation there is always only **one single entity** which is identified as "the" controller.

Consideration should be given to **adding** some definitions to the list contained in the Directive. It would in particular be useful to define the concepts of "***interconnections***" (linking of files); "***anonymising***" \ "***pseudonymising***" and "***blocking***" - which are defined in several national laws.

If a ***procedure*** for clarifying definitional and other issues were to be created, ***the basic definitions can be simplified***, in that the examples and clarifications which are now included in the Directive can be added through that other mechanism - and through that mechanism other clarifications, not yet included in the Directive, can be added. This would both make the Directive more flexible - which is an important general issue - and fit in better with the legislative techniques of some Member States.

- o – O – o -

2. Definitions in and application of the laws – detailed findings

2.1 personal data

> "'**personal data**' shall mean any information relating to an identified or identifiable natural person (***'data subject'***); an ***identifiable person*** is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." (Art. 2(a) of the Directive)

The laws in most of the Member States which have implemented the Directive define the concept of "**personal data**" substantially in accordance with the (basic) definition in the Directive, set out above. This can be said to be the case in Belgium, Denmark, Finland, Germany, Greece, the Netherlands, Portugal, Spain, Sweden and the UK. The proposed new (amended) law in France also contains a (new) definition of "**personal data**" on the lines of the Directive, albeit with some differences, as noted below.

The laws in some of the above-mentioned countries (Greece, Denmark, Sweden and Spain) do not provide the detailed clarification provided by the Directive on what is to be regarded as an "***identifiable person***" - but this would appear to be mainly a matter of legislative drafting technique: as further discussed below, the clarification regarding persons who can be identified "directly or indirectly" is read into these laws too. The proposed new law in France refers to "natural persons ... who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to [that person]" - i.e. the law does not spell out the kinds of factors mentioned in the Directive, but on the other hand does not use the term "in particular". The proposed new law also no longer expressly mentions that the concept of "personal data" covers **data** "***of whatever form***" (as it is put in the current law) - but in practice that remains the case, as noted below.

The law in the UK makes a formal distinction between "**data**" and "**information**" which complicates the terminology used in the law, but has no material effect. More significant is the fact that the law in that State, rather than referring to data which can be linked "directly or indirectly" to a specific individual, refers to *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*". When the law was reviewed by the Government in the context of its so-called "Data Protection Act 1998 – Post-Implementation Appraisal", several interested parties said they has difficulty with this definition: "*For example, how could controllers tell whether identifying particulars were 'likely to come into' their possession?*" The current (pre-implementation) data protection law in Ireland takes the same approach as the UK law, by defining "personal data" as "*data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information which is in the possession of the data controller*" - but the proposed new law adds to this the words "***or*** **[**which**]** ***is likely to come into*** [the data controller's possession]"[6] In other words, the new law (if adopted in its current form) would

[6] The proposed new Irish law defines "**data**" as "*information in a form in which it can be processed*"; defines "**automated data**" and "**manual data**" separately; and adds that "'**data**' *means automated data and manual data*". Put simply, "**automated data**" are data that are, or are intended to be, processed by automatic means; and "**manual data**" are data that are, or are intended to be, held in a non-automated "structured" filing

bring the text of the definition of "personal data" in Ireland in line with the UK law - rather than with the Directive. However, in that respect it must be noted that the new Irish law also contains a provision according to which "*a word or expression that is used in this Act [i.e. in the amended, new law] and also in the Directive [Directive 95/46/EC] has, unless the context otherwise requires, the same meaning in this Act as it has in the Directive*." This should ensure that in practice, in spite of textual differences, the Irish definitions are applied in accordance with the Directive.

On a different point, the law in Portugal expressly adds that "**any information**" means "[***information***] ***of any kind, irrespective of the kind of medium involved, including sound and image*** [***data***]". The law in Luxembourg, too, stresses that the concept covers "***information of any kind, irrespective of the medium on which it is stored*** [F: *support*], ***including sound and image [data]***". In France, too, it has long been held that ***sound and image data*** constitute personal data if they are held in digital format and can be related to an identifiable individual.[7]

As further noted below, the law in Finland expressly states that it applies not just to information on an individual, but also to information on a ***family*** or ***household***.

More problematic is the fact that the laws in Austria, Italy and Luxembourg extend the concept of data subject to **legal persons**. This means that, in these countries, the restrictions on the collecting, storing, disclosing etc. of data on natural persons (in principle) also apply to legal persons, and that legal persons can (again, in principle) exercise the rights of data subjects. Here, the definitional differences lead to clear **divergencies** in the application of the law - as further discussed below, at 3.2.

The other main issue related to the definition of "personal data" is the question of whether this concept is **relative**. One can read the definition in the Directive as suggesting that any data which conceivably can be linked to an individual (in whatever way, and by whoever) are to be regarded as "personal" (even if one may make concessions, or apply the rules in a more relaxed way, if this possibility is somewhat remote). Or one could read the word "***can***" as a reference to the capabilities of any particular person or organisation who or which might have access to the data: the data are then "personal" for someone who (or some organisation which) "can" link the data to an identified individual, but not for someone who cannot establish such a link.

The first approach has the advantage that the legislator and the supervisory authorities retain a "grip" on the data: the data do not "escape" the regulatory framework entirely merely because they are being passed on (indeed, traded) in encoded form. The second approach has the advantage that it does not extend (often onerous) duties, imposed by data protection laws, to persons and organisations who or which process personal data which they have no intention of, and indeed no means of, linking to specific individuals. Indeed, sometimes it will be impossible for persons who process encoded data but who do not have access to the "key" to comply with such duties (e.g. as concerns the informing of data subjects who they cannot contact).

---

system (as further discussed below, at 2.3). While somewhat different from the UK law (and with less effect on overall terminology), this again has no material effect.

[7] See the report *Voix, Image et Protection des Données Personnelles*, CNIL, 1996, also for a wider discussion of the issues.

The issue is not clearly resolved in the Directive. The other language versions are equally ambiguous in this respect (e.g. F: *peut*; D: *kann*; etc.). However, the 15th Preamble can be said to suggest an approach. This Preamble (which deals with ***sound and image data***) reaffirms first of all that processing of such data is only subject to the Directive if that processing is automated or if the data are contained (or intended to be contained) in a "personal data filing system" - but it then adds the words "*so as to permit easy access to the personal data in question*". This can be taken as hinting at the "**relative**" approach: a person who does not have the means to link particular sound and image data to a natural person (or who can only make this link with difficulty) does not have "(***easy***) ***access***" to the data in "***personal***" form.

This would also appear tot be the approach taken by most of the Member States. The Luxembourg law specifically stipulates that it applies to "**the capture, processing and dissemination of sound and image data *which permit the identification of natural or legal persons***" (on the applicability of the law to legal persons, see below, at 3.2). The laws or formal clarifications or interpretations of the laws in Austria, Germany, Greece, the Netherlands and the UK make clear that, in those countries, **encoded or pseudonymised data** are to be regarded as "**personal**" with regard to ***a person who has access to both the data and the "key"***, but not as such 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 separate definitions of pseudonymised data etc.: see below, at 2.9). The term "personal data" is also regarded as relative in Portugal. In Ireland, the data protection authority already (under the current law) takes into account ***the likelihood of a particular person being able to identify a person from data in his or her possession***, and the words added to the definition in the new law, noted above, reinforce this approach - but the Commissioner would be cautious in its application, to ensure that data subjects are not deprived of protection.

Belgium has formally taken the other approach, at least as far as encoded research data are concerned, in that it has adopted **detailed rules on the processing for research purposes of *fully-identifiable-***, ***encoded-*** (*pseudonymised-*) and ***fully-anonymised data***. The laws in Denmark, Finland, France, Italy, Spain and Sweden are ambiguous in this respect (like the Directive), but the authorities tend to agree with the Belgian approach and *in principle* regard all data which still *can* be linked to an individual as "personal", even if the data are processed by someone who cannot make that link. However, they are willing to be **flexible** (less demanding) with regard to the processing of not-immediately-identifiable data, in that the question of whether (and if so, to what extent and how strictly) the law applies is ***related to the probability of the data subject being identified***, with the ***nature of the data also being taken into account***. The more sensitive the data, the closer the data protection authority will examine the likelihood of the data becoming identifiable, and thus the need to apply the law.

The Danish authorities thus had to rule, for instance, on a case involving the transfer of encoded data to a non-EU\EEA country, and held *inter alia* that, because the data were encoded, "adequate" protection was ensured even though the law in the third country concerned did not as such offer protection. They also recognise that with regard to **sound and image data** in particular this is not a clear-cut issue, because it would make all pictures which *can* be recognised by means of face-recognition software "personal data". In that respect, they will therefore make the applicability of the law ***dependent on the circumstances and the likelihood of persons being recognised***.

> CASE EXAMPLE: In a case in Denmark, the data protection authority ruled that a pub which wanted to install "**webcams**" and release pictures from the pub directly on the Internet could not do so without the ***express consent*** of the data subjects, because there was a substantial chance that people in the pub would be recognised. They did not accept the pub's argument that patrons could be said to have consented to this processing of their data by entering the pub in the knowledge that such cameras were installed. The authority felt that such consent should be obtained explicitly, e.g. in the context of individuals signing up for membership (on the question of consent generally, see below, at 6.2).[8]

The two seemingly different approaches also turn out to be less different if one takes into account (as is done in Portugal for instance) that the act of ***anonymising*** of data itself constitutes **processing**. This means that a controller who intends to disclose encoded data must fulfil the requirements for lawful processing in respect of this act. Thus, in Portugal, prior consent is required for the ***encoding*** of sensitive data intended to be disclosed in encoded form for scientific research, even though the data once disclosed in that form are not (no longer) regarded as "personal" as far as the processing by the recipient (the scientist) is concerned. In France, too, detailed rules are in place concerning the anonymising or pseudonymising of data for research purposes, as further discussed below, at 5.3.

The issue is related to a further, increasingly important matter: the use of **data which relate to an object which is not a person** but where the object itself does relate to a person (such as a car, or a house, or a personal computer), and the use of **statistical data** with regard to a person. Sometimes, the relationship between an object and its owner or registered keeper is so close that the data on the object are invariably regarded as data on the person: data on ***car licence plates***, and ***IP-addresses linked to a particular PC*** are thus everywhere treated as personal data. In other contexts, the issue is less clear. Thus, for instance, most people would agree that a ***photograph of a street with houses*** (and not showing people) does not contain personal data. However, a systematic collection of such photographs, with ***links to individual owners or occupiers*** would constitute such data. Again, the line is not an easy one to draw, as the following examples may illustrate:

> CASE EXAMPLE: In the Netherlands, the data protection authority has held that pictures of properties (which are ***systematically collected*** by a company in a major database covering all Dutch streets through ***360º digital pictures***) constitute personal data if they are ***used in such a way as to have repercussions for individuals*** (such as owners or occupiers), e.g. if they are used for valuation or taxation purposes (on the use of image data, see further below, in Part II).

> CASE EXAMPLES: Also in the Netherlands, it was held that while IP-addresses are usually to be regarded as "personal data", a CD-ROM, sold by a company, which linked IP-addresses merely to the ***country*** where the user was based (so that web hosts could use the appropriate language) did not contain "personal" data. [9] Similarly, in France, an Internet access provider is deemed to hold personal data if its data link an IP-address and a user, but not if such links are not retained.

---

[8] Note also a case in Ireland concerning the release on the web of photographs of athletic events, given below, at 10.1, as an example of a case raising issues concerning freedom of expression.

[9] On a more contentious use of information linking an IP address to a particular geographical position, see the Washington Post report of 5 January 2002 "*Bye-Bye Borderless Web: Countries Are Raising Electronic Fences*", referred to below, at 4.2.

> CASE EXAMPLE: In Sweden (as elsewhere) a **telephone number** is normally regarded as "personal data". However, in one case under the previous law it was held that a file with telephone numbers did not constitute a file of personal data as more than one specific person used each telephone. Although this is a rather old case, it would probably be decided in the same way under the new Law.

The reference to ***family*** or ***household data*** in the Finnish law, noted above, must also be read in the sense that such data are "personal" with regard to any member of the family or household in question in respect of which they are used (or if they are used with respect to the family or household as a whole) - but not otherwise. The above-mentioned countries would all agree with this. But again, the line blurs when data are further and further removed from specific individuals. Thus, **postcode-** or **statistical data** by their nature do not relate to individual individuals but to a group of individuals. They indicate that out of a particular group a certain percentage meets a certain criterion: e.g., that 60% of men in a certain age group drink beer on a Friday; or that 90% of the population in a particular district belongs to an ethnic minority; or that 80% of pupils at a particular school are Roman Catholic. Such data are (in the view of all the Member States) ***as such not "personal data"*** - but there is again a "grey area". Thus, some areas of Scotland are so sparsely populated that the postcode covers only a very few households - reportedly, in rare instances, just one household. In France, the data protection authority feels that statistical information on less than 10 results should be reported simply by indicating "less than 11" rather than by a more precise breakdown, which could result in the identification of individuals (see also below, at 5.3, as concerns processing for research purposes).

Also, if one **applies** such statistics to an individual, they do become "personal data" e.g. if one takes such statistics into account in deciding on credit limits (called "red lining" if done by reference to a geographical area); or in excluding people from a list of applicants for a job. The question then becomes whether such data are sufficiently "accurate" to fulfil the "data quality" requirements, discussed below, at 5 - but that is a different matter.

> CASE EXAMPLE: A financial institution in France denied access to a data subject to its segmentation- ("**credit-scoring**-") **criteria** on the grounds that these criteria did not constitute "personal data", but was ordered by the data protection authority to provide the information. On appeal, the courts confirmed that such criteria constituted "personal data" when applied to a specific individual, and that the data subject had a right of access to the information. (The question of whether the criteria were adequate or relevant was not addressed in the proceedings).

2.2 processing

> "'**processing of personal data**'(*'**processing**'*) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, ***disclosure*** by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." (Art. 2(b) of the Directive)

The laws in the Member States all contain definitions which are at least close to the one set out in the Directive - but with a significant amount of minor and not-so-minor variations,

omissions or additions. Thus, the laws in Belgium, Luxembourg, the Netherlands, Portugal, Sweden and the UK follow the text of the Directive *verbatim* (including the ***examples*** given after the word "such as" and the definition-within-the-definition of "***disclosure***").[10] The definition in the proposed new (amended) French law also adds those examples and contains that definition-within-a-definition; otherwise too, it stays very close to the definition in the Directive.[11]

The law in Finland repeats the basic definition and gives the examples of operations which are included in the Directive, but without clarifying the concept of "***disclosure***"; while the law in Denmark only gives the basic definition without the examples (and thus also without the definition of "***disclosure***"). By contrast, as further noted below, at 2.9, several countries add definitions of the term "***interconnection***" (F: *interconnexion*: the terms used in the French language version of the Directive, where the English text uses "combination"), which emphasise that the creation of ***links between databases or files*** also, inherently, involves disclosures. The new law in Ireland, if adopted in its present form, also follows the text of the Directive closely, but refers to both "***collecting***" and "***obtaining***", and adds "***keeping***" of data.

The laws in Austria and Germany use a range of terms, partly retained from the earlier laws. Thus, the Austrian law uses the German term for "**processing of data**", used in the Directive, *Datenverarbeitung*, but also refers to closely-related (and somewhat overlapping) concepts: *Datenanwendung*, *Datenverwendung* and *Handhabung von Daten einer Datenanwendung*.[12] The Austrian law also uses two different terms for **disclosures of data to third parties** (*Übermitteln von Daten*) and **disclosures of data to processors** (*Überlassen von Daten*); while the Italian law uses two different terms for **disclosures of data to *identified* [third] parties** (*comunicazione*) and **disclosures of data to *unidentified* [third] parties** (*diffusione*). The German law uses the term "**processing**" in basically the same sense as the Directive, with some elements of the concept being separately defined (but in accordance with the Directive) - but limits the concept of "**disclosure**" to transmissions (or on-line "making available") of data ***to a third party*** (unlike the Directive which clearly regards dissemination to others than third parties as also constituting disclosure: see the definition of "recipient", below, at 2.7).

---

[10] The Luxembourg law (in its French language version) adds the word "*la*" to the word "*diffusion*" (dissemination), which would suggest that (other than in the Directive) "dissemination" is a separate form of processing, rather than a sub-category of "disclosure" - but I assume that no difference with the Directive is intended.

[11] The definition of "***automated processing***" in the current French law already extends to "***similar operations***" related to (structured) manual filing systems (*fichiers*) and in practice the concept is already applied in a manner similar to the one used in the Directive - although there could be marginal differences. Thus, in a 1994 case, a French court held that using a PC merely to create a list on the basis of paper documents did not constitute "processing" under the 1978 Law. This could be different under the proposed new law - but the question of whether the law (any national law) implementing the Directive shoud apply fully to such marginal use of computers arises as much under the Directive as under the previous law. For instance, the Swedish authorities have raised the question (somewhat rethorically) of whether one should inform a person of the fact that one is drafting a letter to him, and have proposed an exception with regard to draft documents in "running text". In practice, all the authorities take a relaxed view of such matters, and apply the law to such processing if they deem this is reasonable, but not otherwise. Thus, the kind of list produced in the 1994 case in France would not be regarded as subject to the law in the Member States if it was not retained and used by reference to the data subjects, but more so because in that case the data were not held in a (structured) "filing system" (as discussed below, at 2.3) than because the activities involved did not constitute "processing". Also, as discussed below, at 9.1, the Member States would not normally extend the right of access to such a list unless the controller not only retained it but also actually used it by reference to the individuals concerned.

[12] The confusion is not made less by the fact that what used to be called "*Datenverarbeitung*" is now called "*Datenanwendung*".

On the other hand, the law adds a definition of "***use***" (*Nutzung*) which is wide enough to encompass activities which do not constitute disclosures (as defined in that law), and to bring these within the scope of the law.

All in all, these divergencies may not immediately have major repercussions. Thus, the various operations given as examples in the Directive are also likely to be regarded as forms of processing under the Danish law; the making available of data online is also certain to be regarded as a disclosure under the Danish and Finnish laws; and interconnections are likely to be treated as disclosures also outside Greece, Italy and Spain. The somewhat ideosyncratic and additional definitions in the Austrian and German laws too will in most cases not cause substantial differences in the application of the laws. But these divergencies can lead to unforeseen differences in special instances - and they also make it much more difficult for controllers in different countries to properly assess their legal obligations throughout the Community.

2.3 filing system

> "'**personal data filing system**' (***'filing system'***) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis." (Art. 2(c) of the Directive)

The laws in Belgium, Denmark, Luxembourg and Portugal follow the above definition of "**filing system**" *verbatim*;[13] and the laws in Austria, Greece, Italy, the Netherlands, Spain and Sweden also define the basic concept substantially in accordance with this definition in the Directive. However, the laws in Austria, Greece, Spain and Sweden, as well as the proposed new (amended) law in France, do not add the clarification provided by the Directive as concerns decentralised or dispersed systems; while the law in the Netherlands adds that a data set is not to be regarded as falling within the concept unless the data refer to ***more than one person***; the law in Austria emphasises that the data in a "set" must be accessible by reference to ***more than one criterion***; and the proposed new law in France adds that the data set must not only be "structured" but also "***stable***" (i.e. [semi-] permanent).

The law in Finland defines a "filing system" somewhat differently from the Directive as a set of data "***connected by a common use***" and organised or processed in such a way as to allow for the data to be "***retrieved easily and at reasonable cost***." In an attempt to extend its national provisions no further than the minimum required by the Directive, the UK law 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***". However, as the data protection authority in that country has observed:

> "[This] has resulted in a definition that is complex and difficult to apply in practice. It is an example of where a little more regulation, in terms of a slightly broader definition, would have been 'better regulation'. A definition could then have been produced that is more easily understood and applied by the data controllers. It appears that in practice

[13] In the definition of "personal data filing system", the Luxembourg law refers to "data" rather than "personal data", but this is merely because the law uses the former term as a short reference to the latter one, as is made clear in the definition of the latter.

> many data controllers, uncertain as to the meaning of the definition, are in any case taking a broad view so as to be sure of compliance."

In practice, the authority in the UK (the Information Commissioner) tends to take a (cautiously) flexible approach, not unlike the "relative" approach to the question of what constitutes "personal data", discussed above, at 2.1:

> "The Commissioner recognises that data controllers may find that there are grey areas in determining whether or not certain manual information should be brought into line with the requirements of the Act. it is suggested that in those cases where data controllers are unsure whether or not manual information comes within the definition of data/'relevant filing system' they should make a further evaluation in the nature of a **risk assessment**. Data controllers should consider whether or not and, if so, the extent to which, a decision not to treat the information as being covered by the Act will ***prejudice*** the individual concerned. Where the risk of prejudice is ***reasonably likely*** then data controllers would be expected to err on the side of caution and take steps to ensure compliance."

Somewhat surprisingly, given the problems with the UK definition, noted by the data protection authority in that country, the new data protection law in Ireland (as currently before the lower House of Parliament, the *Dail*) follows the definition in the UK law - rather than the one contained in the Directive. However, in this case the provision in the Irish law requiring a Directive-consistent interpretation of terms, already noted above, at 2.1, should ensure that the term is applied in accordance with the Directive, irrespective of such textual differences.

The law in Germany defines "automated processing" separately from the concept of "**non-automated** [i.e. ***manual***] **data sets**" and defines the latter as any collection of personal data which is "organised in ***similarly structured*** [parts]" and which can be "***accessed and evaluated according to specific criteria***".

In practice, in the **vast majority of cases**, the application of these concepts will be ***similar*** in the Member States. However, occasionally there will be differences. In particular, in Germany, the precise demarcation between similar concepts in the previous laws (*Akteien, Karteien, Dateien*) has been somewhat problematic and the difference between the concept in the amended Federal Law and the Directive could therefore have repercussions. The added stipulations in the Finnish and UK laws could also lead to some "structured sets" of data not being regarded as subject to the laws in these countries, even though they would be regarded as falling within the concept of "filing system", and thus within the law, elsewhere.

There is therefore again a certain **divergence** in the application of the Directive in this respect, albeit probably in fairly marginal matters only.

2.4 controller

> "'**controller**' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law." (Art. 2(d) of the Directive)

In defining the concept of "**controller**", the laws in Luxembourg and Portugal follow the main (first) part of the definition in the Directive, quoted above, *verbatim*, but clarify that where the purposes and means of processing are determined by national laws or regulations, the controler *shall* be designated in the legal rules concerned (and while of course leaving out the references to Community law). The laws in Belgium, Denmark and the Netherlands also follow the main (first) part of the definition in the Directive word for word - but the law in Belgium adds the additional clarification about designating the controller by law as an option, while the laws in Denmark and the Netherlands do not. The law in Sweden too closely follows the first part of the above definition and although it too does not include the addition about controllers being designated by law, examples of such designations can be found in specific laws about data processing in public authorities. The proposed new (amended) law in France defines the controller, in accordance with the Directive, as the person who (alone or jointly with others) determines the "purposes and means" of the processing, adding "***unless otherwise specifically designated by statutory or subsidiary legal provisions***", which in effect corresponds to the Directive.

The other laws all contain minor or more substantial variations on, or departures from, the definition inthe Directive.

Thus, the laws in the UK and Italy define the controller as the person who determines the "purposes and ***manner***" of the processing. The reason for this is unclear. As the UK Information Commissioner (the national data protection authority) put it, rhetorically:

> "What is the intention behind the use of the word 'manner' in the UK law rather than 'means'? If this is not clear all the difference does is introduce uncertainty for data controllers, data subjects and the Commissioner."

On the other hand, the UK law is in fact more specific than the Directive about determining the controller when the processing takes place under a law, while the Italian law neither includes a reference to the controller being determined by law, nor mentions the involvement of "others" (as further discussed below). The law in Spain refers to the controller as the person who determines the "purposes, ***contents and use***" of the processing. While not mentioning the possibility of the controller being determined by law, the law in Spain includes a general requirement that the "persons responsible for the filing system" be identified specifically in the rules which must be published in the Official Gazette for each public-sector filing system. The current (pre-implementation) law in Ireland defines the controller (referred to in the law as the "**data controller**") as the person who "either alone or with others, ***controls*** the ***contents and use*** of personal data". This definition is retained in the new (amended) law.

The Greek law defines the controller as the person who determines the "***scope and manner***" of the processing, but adds the clarification about controllers being determined by Greek or European law in terms closely modelled on the second part of the definition in the Directive.

The Austrian law defines the controller as the person who determines the "**purposes**" of the processing only, without reference to the "means" (or manner, or content, or use) of the processing, but adds extensive clarification (not found in the definition in the Directive) on the role of any "processor" who may be involved in the processing, as further noted below, at

2.5. The Finnish law defines the controller as ***the person or persons for whom the filing system is established*** and "who is entitled to determine the ***use*** of the file, or who has been designated as a controller by a **law**."

The law in Germany changes the terms used from "the entity responsible for recording the data" (D: *speicherende Stelle*) to (more or less) the term used in the German version of the Directive for "controller" (D: *verantwortliche Stelle*), but otherwise builds on the previous definition of that entity as the entity which "***collects, [further] processes or uses***" personal data "***for itself***", or which has this done on its behalf by someone else (i.e. by a "processor").

In spite of these ***seemingly quite wide*** **textual divergencies**, in practice there appear to be few problems about identifying the controller of a particular processing operation. In Ireland, as already noted, the new (amended) law expressly stipulates that the term (and other terms) must be applied in accordance with the Directive - but in spite of the differences in the definitions, **the same person or entity will generally be identified as the controller** under any of the above definitions, in any of the Member States. It may not be neat to have such differences, but the practical implications appear to be limited.

There is a problem, however, concerning the reference in the definition in the Directive to determinations of the crucial matters (purposes and means, or any of the other matters specified) by a person or entity "**alone or jointly with others**". As noted above, many national laws have included this phrase (which was added to the definition by the European Parliament, late in the drafting of the Directive) in their own definition of the controller - but there is a ***lack of clarity*** as to what this reference means. In particular, it could suggest that for some processing operations there can be more than one "joint controller**s**". This however raises a host of problems with regard to the application of many of the provisions in the Directive, which generally assume that there is ***one controller*** for any specific operation, and which requires this controller (*singular*) to ensure compliance with various requirements, such as the informing of data subjects, notification, allowing subject access, etc. etc..

This issue is discussed in some detail in the Explanatory Memorandum to the Dutch law, which identifies ***three different types of joint controllership***, but in the end does little more than to say that the respective responsibilities of the different entities involved must be related to the measure of their involvement in the processing operation - which is not particularly helpful. The Introduction to the new UK law, issued by the data protection authority in that country, notes that:

> "The determinations of the purposes for which and the manner in which any personal data are, or are to be, processed does not need to be exclusive to one data controller. Such determination may be shared with others. It may be shared jointly or in common. 'Jointly' covers the situation where the determination is exercised by acting together. Determination 'in common' is where data controllers share a pool of personal data, each processing it independently of each other. The degree of control exercised by each data controller may vary, in that one data controller may have more control over the obtaining of the personal data and another data controller may have more control over the way that the personal data are used." -

but this comment too does little to clarify the implications of such "joint" or "common" controllership.

The question of "joint control" arises in particular with regard to "interconnected" or "shared" databases. The Portugese data protection authority has accepted the notion in a case concerning a database to which pharmacies in Portugal had access (with different access levels being specified for national and local access), but the case was very rare (the issue arose in only one other case) and again does not really clarify the general concept or approach.

The sharing of databases should be distinguished from the making available of data held by one controller, for the benefit of another entity (which constitutes a "disclosure": see the definition of "processing", above, at 2.2) - but the situation can sometimes be confusing:

> CASE EXAMPLE: The data protection authority in Ireland examined a case of a person who was offered a credit card by his insurers - but in which it transpired that the insurance company in fact only acted as an agent for a bank, who was the real issuer of the card (so-called "**cross-marketing**"). The authority determined that the bank was supposed to become the controller of the data requested of the complainant, but that the documentation sent to the complainant had been insufficiently clear in that respect. In other words, this was a case involving two entities but only one of which was the controller.

The issue has implications for the determination of the "applicable law" with regard to processing by (or within) groups of companies, when different companies belonging to the same group are established in different Member States.

In order to avoid problems in the future, this matter should be **clarified** - perhaps best, by stipulating that even if the "purposes and means" of a processing operation are determined in consultations between various entities, there should still always be one identifiable, single (overall) controller for the operation.

2.5 processor

> "'**processor**' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." (Art. 2(e) of the Directive)

The concept of "**processor**" is defined in exactly the same terms as are used in the Direcvtive in the Luxembourg and Portugese law;[14] and in effectively the same terms in the laws in Belgium, Denmark, Greece, Italy, the Netherlands, Spain, Sweden and the UK - the main differences in the latter cases being that some either add examples to the kinds of "persons" or "bodies" that can act as processor (e.g. *de facto* associations), or use more general terms without specific examples (e.g. "whosoever ..." or "a person who ..."). The laws in the UK and Ireland state that employees shall not be considered to be processors (but that is the case under the other laws too, even if this is not spelled out), and the Spanish law, oddly, adds the words "***alone or jointly with others***" to this definition (rather than to the definition of "controller", as is done in the Directive and most other laws).

[14] Except that the Luxembourg law again uses "data" rather than "personal data", for the reason mentioned in the previous footnote.

The Austrian law uses somewhat different wording to define the plural "processors" ("who process data, provided to them, to carry out tasks assigned to them") - but this still in effect amounts to the same thing. However, that law also adds that if a processor carries out data ***other than as instructed*** - for instance, on the basis of a legal obligation, or on the basis of professional or ethical rules - the instructed person rather than the original controller (i.e. the person who instructed the processor) is to be regarded as the controller in respect of that other processing.

The laws in Finland and Germany do not define the concept specifically in their lists of definitions. However, the Finnish law refers in the definitions of "third party" and "recipient" (below, at 2.6 and 2.7) to "***someone who processes personal data on behalf of [the controller]***". The proposed new (amended) French law refers to a "***processing agent***" (*sous-traitant*) in its (somewhat odd) definition of "recipient" (also discussed below, at 2.7) and stipulates in the rules on processing by such agents that the term covers "***anyone who processes personal data on behalf of the controller***". And the German law deals in some detail with processing "on one's own behalf", or "on instructions" - and in the latter context also uses the general term for "***agent***" (*Auftragnehmer*; the controller\principal is thus the *Auftraggeber*). The latter has the advantage that it makes clear that what the Directive calls a "processor" is nothing different from what is regarded as an agent in other legal contexts (in particular in civil law). Since consistency in law is to be welcomed, and since in most other Member States a similar approach is likely to be taken if the question arises, it might be useful to clarify explicitly that this is the appropriate interpretation. However, in Ireland and the UK the concept of an "agent" has a very particular legal meaning and may therefore not always coincide with the concept of processor.

2.6 third party

> "'**third party**' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data." (Art. 2(f) of the Directive)

The concept of "**third party**" is defined in exactly the terms used in the Directive in the Luxembourg and Portugese laws; and in basically identical terms in the laws in Belgium, Denmark, Finland, Greece and the Netherlands (the only minor differences being again that some either add examples to the kinds of "persons" or "bodies" that can act as processor (e.g. *de facto* associations), or use more general terms without specific examples (e.g. "anyone ..." or "a person who ..."). The Luxembourg law adds (after the definition as set out in the Directive) that in the public sector, public bodies (ministries, public enterprises, local authorities, etc.) other than the one designated as controller (see above, at 2.4) are to be regarded as "third parties". The law in Sweden also follows the text in the Directive, but expressly adds the [in-house] data protection official to the list of persons who are not included in the term, while the law in the UK refers, not to persons who process data "under the direct authority of the controller or the processor", but to persons "***authorised to process data* for *the data controller or processor***" - which is pretty much the same thing.

The concept of "third party" is not specifically defined in the laws in Austria, Ireland, Italy and Spain. However, the Spanish law specifically refers to "third parties" (*tercero*) in the provision on disclosures; and the Austrian law (as noted above, at 2.2) distinguishes between

two types of disclosure, with one of these clearly (though not expressly) referring to disclosures to third parties. The Italian law refers to (identified\specific) "parties other than the data subject" - but while this clearly includes "third parties", it is best read as referring to what are called "recipients" in the Directive (i.e. as including recipients who are not "third parties" such as recipients within the organisation of the controller: see below, at 2.7). The German law defines the concept of "third party" basically in accordance with the Directive - but limits the reference to parties not to be considered "third parties" to data subjects and "persons ***in Germany or in the EU\EEA*** who carry out processing on instructions". This means that under the German law processors outside the EEA *are* considered to be "third parties". It follows from this that more stringent conditions can be placed on transfers of data to such non-EU agencies than can be imposed on transfers to processors within the EU - but that would not appear to violate the Directive (as further noted below, at 14.3).

The proposed new (amended) law in France contains a single definition of "**recipient**" (*destinataire*) which, however, appears to draw mainly, and confusingly, on the definition of "***third party***" in the Directive, as discussed in the next section (section 2.7). That confusion aside, one can however perhaps deduce from that definition that "the data subject, the controller, the processor and the persons who, because of their functions, are authorised to process the data" (as referred to in that definition) are not "third parties".

2.7 recipient

> "'**recipient**' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients." (Art. 2(f) of the Directive)

The Portugese law again follows the definition in the Directive *verbatim*. Otherwise, the basic definition of a "**recipient**" as ***anyone to whom data are disclosed*** is contained in the laws in Belgium, Denmark, Germany, Greece, Luxembourg, the Netherlands, Sweden and the UK - but there are ***significant differences*** when it comes to the additional clarifications of the term. Thus, only the laws in Denmark and Luxembourg add, in so many words, both the additional clarification contained in the Directive that this includes ***both third parties and others*** and the somewhat odd stipulation that ***authorities who receive data in the framework of a particular inquiry*** shall not be regarded as recipients (the Luxembourg law, in the latter context, refers to a "***statutory investigation or supervsion***" [F: *une mission légale d'enquête ou de contrôle*"], but that is pretty much the same thing). The laws in Belgium, Greece and the UK also explicitly contain the first clarification (with the UK law going into somewhat more detail); the extension of the concept to others than third parties also clearly follows from the German law (because of the immediately following definition of "third party"); and this matter can be read into the laws in the Netherlands and Sweden too.

However, there is clearly unease as concerns the exclusion of "***authorities which may receive data in the framework of a particular inquiry***" from the concept of "recipients". In Denmark, the exception has never been invoked; and the clause has of course also not yet been relied on in Luxembourg since the law itself has not yet come into force. The laws in Germany, Greece and the Netherlands do NOT contain this exclusion, while the Belgian law limits it to "administrative and judicial authorities"; and the Swedish law limits it further to the providing of data to an authority "***in order that [the] authority should be able to perform***

such supervision, control or audit as it is under a duty to attend to." By contrast, the UK law ***elaborates*** on this exception by applying it to "***any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law***."

As already noted above, at 2.6, the proposed new French law contains a definition of "**recipient**" (or to be more precisely, if rather oddly, of "***recipient of a personal data processing [operation]***") which covers "***any person authorised to receive communication of [such] data other than the data subject, the controller, the processor and the persons who, because of their functions, are authorised to process the data.***" This suggests that - contrary to the express stipulation in the Directive - the data subject, the processor and employees of the controller are not to be regarded as "recipients". If adopted in its present form, this would create substantial differences between that law and the laws of the other Member States which implement the Directive more faithfully.

The concept of "**recipient**" is not specifically defined in the laws of Austria,[15] Finland, Ireland, Italy and Spain - although the reference in the Italian law to disclosures to "identified parties other than the data subject" (contained in the special definition of disclosures to such parties, discussed above, at 2.2) must be read as referring to "recipients", as was already noted above, at 2.6. With regard to these countries, this means that the exception concerning disclosures to authorities in the framework of a particular inquiry is also not endorsed. Rather, such disclosures must - in these four Member States as in Germany, Greece and the Netherlands be assessed by reference to the ordinary rules on processing and\or to any special rules on disclosures, more in particular by reference to any special rules on disclosures to public authorities in connection with "monitoring, inspection or regulatory functions", discussed below, at 10.3.

The use of partially different (or incomplete) definitions here thus clearly leads to **divergencies in the application of the laws**.

2.8 consent

> "'**the data subject's consent**' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." (Art. 2(h) of the Directive)

The vast majority of the Member States define the data subject's "**consent**" in accordance with the Directive. Indeed, no less than eight - Belgium, Denmark, Finland, Greece, Luxembourg, the Netherlands, Portugal, Spain and Sweden - do so in terms which repeat the above *verbatim*, albeit sometimes with some **additions**. The Spanish and Swedish laws add the requirement that consent must be "***unambiguous***" to the definition (rather than to the substantive provisions concerning processing on the basis of consent, as is done in the Directive); while the Luxembourg law adds that consent must be "***explicit***" and "***unambiguous***" (as well as "free, specific and informed") - which has repercussions for the application of the consent "criterion", as further noted below, at 6.2. The Greek law adds detail about the information that has to be provided. And both the Luxembourg and the

[15] Note in particular that the concept of "recipients of disclosed data" (*Übermittlungsempfänger*) in the Austrian law only refers to ***third-party recipients***.

Belgian law add that consent can be given by a data subject's "***legal representative***" (read: if the data subject is physically or legally incapable to give his or her own consent).

The definition of consent in the Austrian, German and Italian laws are also very close to the definition in the Directive, in that they all require that consent must be free, specific and informed, with the Italian law adding that such consent must (always) be given ***in writing***, and the German law requiring this in principle, and adding that if consent is obtained for purposes which are different from the main purpose for which the data are collected, the request for the separate consent must be ***clearly distinguishable*** from the consent for the main purpose of the processing.

By contrast, the UK law ***does not define*** "**consent**" ***at all*** - and some provisions in the law suggest that consent can in fact be ***implied*** (rather than having to be "signified"). The data protection authority also relates the nature of the consent required to the circumstances (although elsewhere she expressly refers back to the Directive in her guidance on the law):

> "In some cases, **implied consent** may be sufficient. In others nothing less than **clear written consent** will suffice."

The Irish law, too, does ***not define*** consent - but the term is there less likely to be applied in such a relative lax way, if only because of the stipulation (already noted in earlier sections) that terms used in the law and the Directive must be applied in accordance with the latter instrument. The discussion in that country on the phrasing of the consent "criterion" for lawful processing, further noted below, at 6.2, also suggests that a strict view is likely to be taken of this matter.

Neither the current nor the proposed new (amended) French law define the concept of "consent". The current law only refers to consent in the context of processing of "***sensitive data***", for which the law requires "***express***" consent, which means that it has to be ***in writing*** (subject to some concessions with regard to processing on the Internet, as discussed below, at 7.2). The proposed new (amended) law refers to "**consent**" (without qualification or clarification) in the relevant general "**criterion**" for lawful processing (as discussed below, at 6.2), and retains the requirement of "***express consent***" with regard to the processing of "***sensitive data***". In practice, as further discussed in the sections just mentioned, it is certain that **consent** for the processing of ***non-sensitive data*** will only be regarded as valid if it amounts to a "***freely given, specific and informed*** indication of" the "wishes" (*volunté*) of the data subject; while **consent** for the processing of ***sensitive data*** will still have to be "***express***" and thus ***in writing*** (subject to the concessions with regard to processing on the Internet).

Overall, there is therefore **very substantial convergence** (indeed, ***equivalence***) between the continental-European States on the basic definition of consent - or at least, on its application in practice (with Italy and Germany adding requirements about the ***form*** in which consent must be given). However, the UK somewhat **diverts** from this consensus by not defining the concept at all and accepting "implied consent" in some circumstances; and the situation in Ireland is still somewhat **unclear**.

2.9 additional definitions in the laws of the Member States

All the laws except for the Belgian law contain definitions in addition to the ones contained in the Directive and discussed above. Some of these are merely short references, e.g. that "***the Authority***" shall mean the national data protection authority established under other provisions of the law, or that "***prior check***" shall mean the special procedure envisaged in Art. 20 of the Directive, as reflected in the law concerned. The laws in Austria, Germany, Greece, Ireland and the UK also specifically define the concept of "***sensitive data***", by which they mean the "special categories of data" regulated by Art. 8 of the Directive, as further discussed below, at 7 (where it is noted, at 7.1, that the laws vary to some extent in regard to these categories). The Luxembourg law defines "***health data***" and "***genetic data***", as also further discussed below, at 7. The Danish, Luxembourg and Swedish laws define the concept of "***third country***", which is used in relation to the question of "applicable law" and cross-border data transfers, as further discussed below, at 4.1 and 14.1 (where it is noted that the Member States differ in this respect too, with some of them regarding the non-EU EEA States as "third countries" while others treat them as, or on a par with, the EU Member States).

Some laws also add definitions of more specific **aspects of processing**, such as ***collecting*** (with the UK law, for instance, making clear that this includes all *obtaining* of data, while the Austrian law limits the concept to collecting of data *with a view to systematic processing*), or make further distinctions between various categories of ***disclosure***, ***communication*** or ***dissemination***, as was noted above, at 2.2.

Some laws add definitions specific to the one Member State. Thus, the German law defines a "**mobile data carrier**" (which includes "***smart cards***" in particular); the Finnish law defines "**personal credit data**" (because of certain special rules on the processing of such data, set out in the context of processing of sensitive data, as further discussed below, at 7); the Luxembourg law defines "**surveillance**" (and adds rules on processing for the purpose of surveillance, further discussed below, at 10.4); and the Spanish law "**sources accessible to the public**" (because of certain special rules on the processing of such data, as discussed below, at 10.1). The UK law contains more than 40 (!) definitions. Many of them are short references ("the Commissioner", "the Data Protection Directive", "Minister of the Crown", etc.); some define concepts by reference to various domestic laws and regulations ("school", "pupil", "health professional", etc.); and some are really interpretations of certain terms (e.g. the clarification of how the term "accurate" should be applied, as discussed below, at 5.1). The Irish law also contains a long list of short references and cross-references ("appropriate authority", "the Commissioner", "company", "financial institution", "local authority", etc.), and makes clear that the term "**direct marketing**" includes ***direct mailing***.

A number of concepts stand out. Thus, the laws in Austria, Greece, Luxembourg and Portugal add definitions of (respectively) "**linked data files**", "**interconnections**" and "**combination of data**" - which are important because such linking of files is widely regarded as inherently risky and in any case inherently involving ***disclosures***. The proposed new (amended) French law also clarifies the concept, in the context of stipulating "***prior checks***" for "**interconnections**".

The laws in Germany, Ireland, Italy and Sweden add definitions of "**blocking**". The German and Irish laws clarify that this involves "***marking***" the data in such a way as to ***prevent processing*** or making it ***not possible to process [the data] for purposes in relation to which it***

is marked; the Italian law refers to the "***temporary suspension***" of processing; while the Swedish law refers to "***restrictions***" on the use of "blocked" data, and in particular on the ***disclosure*** of such data (while adding a rather dubious exception which says that "blocking" shall not prevent disclosure under the Freedom of the Press Law - which is the Swedish law guaranteeing access to official documents - as further discussed below, at 10.2). The Greek law too makes clear (albeit in the briefest possible way) that "blocked" data are to be "***locked***" so as to prevent their use.

Several laws define "**anonymising**" or "**pseudonymising**" (***encoding***) of personal data. The Austrian law uses the phrase "[only] ***indirectly identifiable data***" to describe what others call "peudonymous data", in that it defines it as data which the person processing the data ***cannot link*** to an (identified) individual "by lawful means" (which is somewhat confusing because other Member States use these words to describe data which ***can*** be linked [lawfully] to an individual, such as a national identity number). The German law defines "**anonymising**" of data as "the altering of personal data in such a way that the data ... can ***no longer be linked*** to an identifiable person, or can ***only be linked to such a person through a disproportionate effort in time, costs or labour***", and "**pseudonymising**" as "the replacing of a [data subject's] name or other personal characteristics with a mark [read: code or number] with a view to ***making the identification of the data subject impossible or substantially more difficult***." These definitions show that the concepts are by no means clear-cut and indeed blend into each other. By contrast, the Spanish law refers to "**anonymising**" (which it calls a "**dissociation procedure**") as "processing of personal data carried out in such a way that the information obtained ***cannot be associated with an identified or identifiable person***." The Italian law similarly defines "**anonymous data**" as "***any data which in origin, or by its having been processed, cannot be associated with any identified or identifiable data subject.***"

Consideration should be given to either **adding** some of these definitions - in particular of "blocking" and "anonymising"\"pseudonymising" - to the list of definitions in the Directive, and\or to **clarifying** relevant matters - such as what exactly constitutes a "disclosure" (in particular in the context of "interconnections" of files or databases) or what the implications of "blocking" are - in the guidance which it is proposed should be issued with, and under, the (revised) Directive (see below, in Part III).

- o – O – o -

3. the substantive scope of the laws [Arts. 3 & 5]

introduction

The Directive requires the Member States to apply its provisions (through their national laws) to all **automated processing** of **personal data** and all processing of such data involving **"structured" manual files**, as far as processing **within the scope of Community law** is concerned (and with certain matters being "in any case" excluded). The study examined to what extent the Member States have limited themselves in these regards, or where they have applied their laws more widely to ***deceased persons***, ***legal persons***, or ***matters outside the scope of Community law or the Directive***.

It also looked at ***the relationship between the national laws implementing the Directive and other domestic legislation***.

summary of findings

The Member States all apply their laws to processing by means of both **automated and "structured" manual systems**, but some 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, noted in the previous section. As a result, **some divergencies in application** remain in spite of a ***large measure of convergence on paper***.

Several Member States extend ***some*** protection to data on **deceased persons**, but under other, more general legal rules rather than under the laws implementing the Directive. In addition, three Member States extend protection ***quite generally*** to **legal persons**, and one to ***certain data on such persons*** (while another one or two could possibly apply some limited protection under more general legal concepts). In that respect, there are therefore clearly **substantial divergencies** between the Member States.

The laws in all the Member States apply, in principle, "across the board", to ***matters both within and without the scope of Community law*** - even though they also often contain quite sweeping exemptions and exceptions concerning typical "Third Pillar" matters such as police- or state security matters.

Finally, the **status** of the 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 all***

other legal provisions, while in others, the precise status and relationship with other laws is **unclear**. As a result, **the upholding of the standards in the Directive is not universally guaranteed**, even with regard to matters within the scope of Community law.

matters to be further clarified or addressed

The differences in scope between the laws of the Member States have implications in particular in connection with **transnational activities**, as further discussed below, at 4 and 14. Here, it may suffice to note that the application of (parts of) some laws to **legal persons** is not ***contrary to the Directive*** (as is clear from the 24th Preamble), but nevertheless ***raises wider issues*** to be addressed in the context of the revision of the Directive.

As far as the extension of the laws of the Member States to matters **outside the scope of Community law or the Directive** is concerned, it must be noted that this can cause **serious constitutional problems** at Union- and national level if the "***applicable law***" provision or the ***freedom to transfer data within the EU*** are ***uncritically extended*** so as to also apply in matters with regard to which proper data protection is not ensured, as is done in several countries.

The **relative status** of the laws implementing the Directive in the domestic legal systems has implications in particular with regard to ***processing in the public interest or in the exercise of official authority***, discussed below, at 6.3; with regard to the ***processing of sensitive data***, discussed below, at 7; and with regard to the ***exceptions to the normal rules***, discussed below, at 10.

- o – O – o –

3. the substantive scope of the laws – detailed findings

3.1 applicability to automated and manual processing

> "This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system." (Art. 3(1) of the Directive)

The laws in Belgium, Finland, Greece, Luxembourg, the Netherlands and Portugal set out their scope *verbatim* as in the provision of the Directive, quoted above, and the law in Sweden, and the proposed new law in France, also use effectively the same wording (the new French law merely adding the exception concerning "purely personal or household activity" and clarifying that the applicability of the law is also subject to the "applicable law" provision, discussed below, at 4.2). The law in Denmark refers to processing of personal data "with the help of electronic data processing" and to data which "will be held" in a filing system, which is pretty much the same thing. In spite of rather cumbersome wording, the UK law too applies in this respect in accordance with the Directive. The Irish law does not contain a provision on the lines of Art. 3(1) of the Directive, but in practice also applies to all automated and manual processing (or rather, since the core concept in the law is not changed by the proposed amendments, to all personal data processed [or intended to be processed] automatically and to all personal data contained [or intended to be contained] in structured manual filing systems).

The laws in Denmark and the UK **extend** the application of their laws to ***some "non-structured" manual files***. The Danish act also applies to the **"systematic" non-automatic (i.e. manual) processing** of personal data which is performed for private persons or bodies, even if the data are not held in a ("structured") filling system, if the data relate to an individual's "**private or financial conditions or other personal circumstances which can reasonably be expected not to be made accessible to the public**." However, such processing is not subject to Parts 8 and 9 of the Law, which deal with the providing of information to data subjects and with the right of access. The UK law extends its scope to **certain manually-processed health- and educational records** and a long list of "**accessible public records**", irrespective of whether they are "structured" or not.

The German law applies in accordance with Art.3(1) of the Directive when it comes to **private-sector controllers**, but ***more widely*** as concerns **public-sector controllers**, who must comply with the relevant rules in the Law in ***any*** "***collecting, [further] processing or use***" of personal data, irrespective of whether this is done by automated means or involves "structured" files. The law in Italy goes beyond this by make **any processing of personal data** subject to its provisions.

The law in Austria also quite generally applies to **any processing of personal data**, even if some provisions (e.g. as concerns the exercise of data subject rights) only apply to data which are automatically processed or held in "structured" manual files.

The Law in Spain says that it only applies to personal data which are "**recorded**" on a "***physical support***" (read: data carrier) in such a way as to "***allow***" their processing. This could be read as excluding (e.g.) ***transient audio- or video-surveillance*** (i.e. when the sound- and image data are not recorded). However, the term "physical support" is read most widely,

so as to include any kind of equipment - and in practice the words are not applied in such a way as to restrict the application of the law: the Spanish data protection authority thus decided that the mere use of a webcam in the premises of a journal to display through the Internet the images of the workers in the office was considered against the law because of the high possibility these people could be identified through the images taking into account the context in which they were taken.

It must be noted that the application of the various provisions in the laws on the scope of these laws, summarised above, are of course also affected by the way in which the terms used - in particular, "**personal data**" and "**filing system**" - are defined and applied, as discussed above, at 2.1 and 2.3. Even if a law faithfully (or even *verbatim*) repeats Art. 3(1) of the Directive, the law may apply differently from another law using the same terms, if they define those concepts differently. Thus, for instance, the Belgian law applies to ***encoded data*** which are automatically processed or held in a "structured" filing system, while the Dutch law does not apply to such data if they are processed by someone without access to the "decoding key".

The differences in scope resulting from differences in the provisions mentioned above, or from differences in these definitions, have implications in particular in connection with the extra-territorial application of these laws, or conversely their non-applicability when other national laws apply in the State concerned, as discussed below, at 4.1. Here, it will suffice to note that again, in spite of a large measure of convergence, **divergencies** remain.

3.2 applicability to deceased or legal persons

> "This Directive shall apply to the processing of ... any information relating to an identified or identifiable natural person" (Art. 3(1) of the Directive read together with the definitions of "personal data" and "data subject" in Art. 2(a))
>
> "Whereas the legislation concerning the protection of legal persons with regard to the processing [of] data which concerns them is not affected by this Directive;" (24th Preamble)

As noted above, at 2.1, most of the laws of the Member States define the concepts of "**personal data**" and "**data subject**" in such a way as to apply those terms only to "***natural persons***" or "***physical persons***"; and it follows from this that the rules in these laws concerning the processing of "personal data" or of data on "data subjects" also only apply to the processing of information on such persons.

The data protection laws in these countries - Belgium, Finland, France (both the current and the proposed new (amended) law), Germany, Greece, the Netherlands, Portugal, Spain, Sweden and the UK - consequently do not apply to data on ***deceased persons***.[16] Some laws make this explicitly clear by referring to "***natural* living *persons***" or "**living *individuals***" (Sweden and Ireland and the UK respectively). The law in Denmark also simply defines the concept of "personal data" as "any information relating to an identified or identifiable natural person ('data subject')" - but the Explanatory Memorandum to the law says that this should be read as also applying to deceased persons (albeit without further clarifying how long the protection accorded to such people lasts).

[16] The law in France allows relatives of a deceased person to require controllers who have not yet recorded that fact to rectify this omission.

This does not necessarily mean that the processing of data on deceased persons is devoid of any regulation or protection in the countries concerned: in some countries (e.g., Germany, the Netherlands) more general legal rules can have a bearing, and may lead courts in certain cases to impose restrictions, e.g. on the basis of broad legal provisions concerning "improper" acts (NL: *onrechtmatige daad*; D: *unerlaubte Handlung*; cf. the French and general continental-legal concept of *faut*). In Sweden, where no consideration has been given to extending data protection to legal persons *per se*, certain laws nevertheless extend some protection to such persons in certain contexts, e.g. as concerns **confidentiality** (or ***secrecy*** as it is more usually called there) or as concerns **credit data**.

For the purpose of this study it must suffice to note that such data are however not subject to the detailed and specific rules in the laws implementing the Directive.

The laws in Austria, Italy and Luxembourg also do not generally apply to ***deceased persons*** - except that the Luxembourg law does contain a special provision, allowing close relatives of a ***deceased patient*** access to the latter's medical file. However, as already noted above, at 2.1, in those three countries the concept of "data subject" (and thus the concept of "personal data") has been expressly extended to apply to "**legal persons**" and indeed ***associations*** without formal legal personality, as well as to "natural persons".[17] This has not been done in the other countries just mentioned, and in these the data protection laws therefore generally do not apply to legal persons.

However, while not generally considering data on legal entities etc. to be "personal data", the Danish law nevertheless applies to **data on companies and similar commercial legal entities** (DK: *virksomheder m.v.*) if the data are processed by ***credit reference agencies*** *or* ***businesses which warn third parties*** against entering into business relations or an employment relationship with a data subject (blacklisting companies). Part 5 and 6 of the law contains rules concerning credit information agencies and include special rules concerning disclosure of data on debts. The law can be extended by decree to the processing of data concerning companies, etc. which is performed for private persons or bodies and to the processing of data concerning enterprises, etc. performed on behalf of public administrations. The Minister of Justice has decided to use this power in one situation.

Finally, it may be mentioned that although the German law too basically only applies to data on "natural persons", the constitutional provisions which lie at the root of data protection in that country can have implications with regard to the processing of data on "legal persons" too - but this matter has not yet been clarified.

I have discussed the question of applying data protection to "legal persons" in detail in a previous study for the Commission.[18] In that study, I concluded that the application of the laws implementing the Directive to such entities in some countries but not in others creates obstacles to the Single Market. Here, it may be noted that it also complicates the application of the "applicable law" provisions in the Directive, in that it means that sometimes controllers outside Austria, Italy or Luxembourg (or indeed Denmark and perhaps Germany) can find

---

[17] The Luxembourg law exempts from its scope, processing of **data on legal persons and associations etc. which must be made public by virtue of a law or regulation**. On the other hand, as noted above, at 2.1, it expressly includes "**sound and image data**" relating to legal persons (as well as such data relating to natural persons).

[18] See footnote 2, above.

that they have to comply with restrictions on the processing of data on legal entities to which they are not subject in their home country (i.e. if they are subject to the Austrian, Italian, Luxembourg (Danish or German) law), while conversely, controllers in these countries who process data on such entities may find that they are exempt from the local restrictions because they are subject to the law in another EU Member State which does not apply to such data. This is further discussed below, at 4.2.

3.3 applicability to matters within and without the scope of Community law

> "This Directive shall not apply to the processing of personal data ... in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law" (Art. 3(2), first indent, of the Directive)

As is clear from Art. 3(2) of the Directive, quoted above, that instrument *as such* does not apply to matters outside the scope of Community law and "in any case" not to "Third Pillar" matters. However, this is basically because, as an ***EC*** Directive, its scope is inherently limited to matters within the scope of Community law. The limitation stipulated in the Directive is not a natural or very practical one: as the UK Data Protection Registrar (as the data protection authority in that country was previously called) pointed out: "*the boundary* [*between matters within and without the scope of Community Law*] *is unclear; some organisations straddle the boundary*"; and that boundary is also continually shifting. When the Directive was drafted, it was therefore intended to apply the principles of the Directive also to matters outside the scope of the "First Pillar" (albeit through separate instruments); and indeed a range of "Third Pillar" measures have addressed data protection, and data protection is now also ensured for processing by the Community itself. From the point of view of the Member States, applying the requirements of the Directive only to matters within its scope furthermore creates problematic and unwarranted "seams" between data protection regimes in different (but not easy to separate) sectors.[19] It is therefore not surprising that the laws of **all the Member States** which have implemented the Directive so far - Austria, Belgium, Denmark, Finland, Germany, Greece, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the UK - apply, in principle, "across the board", to ***matters both within and without the scope of Community law*** - even though they also often contain quite sweeping exemptions and exceptions concerning typical "Third Pillar" matters such as police- or state security matters, as further discusses below, at 10.3. The same applies with regard to the proposed new laws in France and Ireland.

However, this can cause problems if certain specific provisions in the Directive, which are predicated on the assumption that a more than "adequate", "high" level of data protection is assured throughout the EU, are uncritically applied to matters where this can be in doubt. This can be the case, in particular, with regard to the national provisions on "applicable law", if they generally exempt processing on their territory and\or of data on their citizens from the domestic law if the controller is established in another EU Member State (as they must do for

[19] See my earlier study for the Commission into "*The feasibility of a seamless system of data protection for the European Union*: footnote 3, above.

matters within the scope of Community law), and the law in the other EU State does not provide proper (or indeed any) protection because the non-Community matter in question is exempt from the normal data protection rules in that country. And it can be the case with regard to the stipulation of the "free zone" for data transfers within the EU, if this freedom is extended to transfers in non-Community matters with regard to which the other State does not provide adequate (or indeed any) data protection. Only a few Member States have recognised this problem and included specific rules differentiating between matters within and without the scope of Community law in these respects, as will be noted in the sections dealing with these issues, sections 4.2 and 14.2 respectively.

Here, it must suffice to note that while there are therefore ***no major divergencies*** in this respect between the Member States, this actually means that the **problems arising from the uncritical application of some provisions in the Directive to processing related to matters outside the scope of Community law** are also shared between ***most Member States***.

3.4 relationship with other laws

The relationship between the national data protection laws implementing the Directive and other laws in the same country **varies considerably**, and is not always clearly spelled out. As already noted above, at 1, this matter is, in many countries, **crucially affected by constitutional doctrine**.

In Germany, the Federal Data Protection Law is seen as **the embodiment of the constitutional principle of *"informational self-determination***" (*informationelle Selbstbestimmung*), first enunciated in the famous 1983 *Census*-judgment of the German Constitutional Court - even if its specific terms do not necessarily override more specific provisions in other laws. In Spain, the right to "*libertad informática*" has similarly been confirmed in a recent (2001) Constitutional Court ruling as an independent constitutional right, distinguishable from the right to private and family life. The Austrian law too makes clear, through a so-called "constitutional clause", that its object - data protection - is a **constitutional right**; the law is thus seen as expressing ***generally*** how the **constitutional imperative of data protection** is to be applied in practice. The general data protection law in France is also considered to embody the general constitutional approach in this area, as can be gleaned, in particular, from its broad (one could say, "mission"-) statement in its first article - to be retained without change in the proposed new law - that:

> "*Information technology shall be at the service of each citizen. It shall operate in the framework of international cooperation. It shall violate neither human identity nor human rights, private life, or individual or public freedoms.*"

The point to be made about the constitutional approach in these countries, which has also been adopted in other countries such as Greece, Italy and Portugal (and to a lesser extent in Belgium, Ireland, Luxembourg and the Netherlands) is that it creates a **hierarchy of legal norms**, and requires adherence to certain general **constitutional principles** in any legal rules touching on human rights. Specifically, it means that any rules which limit fundamental rights (including data protection or the rights linked to data protection) must be set out in ***accessible*** (i.e. published) and sufficiently ***precise terms*** (i.e. they must be ***foreseeable***) in a ***formal statute*** (*Gesetzesvorbehalt*); they may not affect the "***untouchable core***" of the right

concerned; and they must be in accordance with the principles of "***necessity***" and "***proportionality***".[20]

In the above countries, other rules relating to data protection must **always** be assessed in the light of these general principles; and the general data protection laws help in that assessment. This does not mean that data protection rules in other laws cannot deviate from the rules in the general data protection law, or that regulatory powers cannot be delegated to lower authorities. I will in fact refer to a range of other laws in other sections of this report, e.g. as concerns processing of data in connection with employment, or research etc. Rather, the point to be made here is that such **other laws, delegating provisions or lower regulations are only valid if they adhere to the above-mentioned principles**. Thus, a recent judgment by the Constitutional Court in Portugal held that a **Decree-Law on video surveillance** was ***invalid*** because such surveillance by its very nature touched on "private life", which is constitutionally regarded as sensitive and can therefore only be regulated by formal statute. The Spanish Constitutional Court similarly held (in the 2001 ruling already referred to) that stipulations in **two articles in the data protection law** were ***unconstitutional*** because they were too broad and could lead to abuse of powers, and failed to meet the above-mentioned principles of accessibility, foreseeability, pressing social need\necessity and proportionality. In various sections, below, the implications of this ruling will be noted. In Ireland, it was held that using the **Public Service Number** (an identity number of wide application in the public sector, further noted below, at 7.6) to facilitate data exchanges between public bodies constitutionally required ***statutory authority*** (which was provided by the adoption of a new special law). The fact that data protection has a constitutional basis in that country also has implications for the application of other laws to which the data protection law may refer or defer, in that it requires the application of a "**legitimate purpose**" and "**prejudice**" test, as further discussed below, at 10.3.

In Greece, the rules in the data protection law are regarded as having **quasi-constitutional status** and as thus being ***formally superior*** to any conflicting rules in other laws (even if this is not as formally stated as in Austria). In Denmark, too, the rules in the data protection law are expressly stipulated to constitute the **basic minimum**: rules which have a bearing on data protection in other laws only apply if they provide a ***higher*** level of protection (however, according to the Explanatory Memorandum to the law, if the lower level of protection in the other law was intentional and not in contravention of the Directive, the rule in the other law will be allowed to apply).

The law in the Netherlands is not given a ***formally superior*** status but does give effect to a constitutional and international norm and is therefore still seen as **setting the standard** to which other laws ought to conform. The special laws on filing systems maintained by the police and the security services are therefore to be brought into line with the general law and

[20] The above principles are also reflected in the case-law of the European Court of Human Rights, and thus given an even wider European basis and effect, equally permeating Community (and Union) law. For an old but simple and still valid overview of the approach by the ECtHR, see D Korff, *The guarantee of freedom of expression under Art. 10 of the European Convention on Human Rights*, in: Media Law and Practice, Vol. 9, Number 4, December 1988, pp. 143 – 150. For a more recent, detailed and academic discussion, see (e.g.) Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights, 1st ed. (1995), Chapter 8 (Article 8 – 11: General considerations), in particular p. 285 ff. On the reflection of these principles in Community law, see (e.g.) Wyatt & Dashwood's European Community Law, 3rd ed. (1993), p. 88 ff (The General Principles of Community Law); Brown & Kennedy, The Court of Justice of the European Communities, 5th ed. (2000), Chapter Fifteen (Fundamental Doctrines & General Principles of Community Law).

the Directive (taking into account the various exceptions that apply to such systems), while data protection rules in other laws are also supposed to be applied in accordance with the law and the Directive from now on. The Italian law contains some wide exceptions for some (not all) police and security services files, but is otherwise similarly regarded as **laying down the constitutional standards** to be applied ***generally***. It allows processing on the basis of other laws, but in this nevertheless reflects the constitutional approach in stressing that processing on that basis must be required (read: necessary) for the task concerned and that the processing of personal data on that basis must always be minimised and based on respect for the constitutional principle of privacy (or "personal secrecy").

In Belgium, the precise status of the law implementing the Directive in relation to the other laws is not entirely clear, but that law is nevertheless regarded as of **constitutional importance** and thus as at least giving ***guidance*** on how to interpret and apply relevant provisions in other laws. In Finland, the data protection law is perhaps not quite seen in this light, but **all the other relevant laws and legal provisions** are nevertheless also being ***reviewed*** in the light of the Directive.

The Luxembourg law stipulates that with regard to **public security**, **defence**, the **investigation and prosecution of criminal offences** and **State security** (including ***economic and financial matters*** related to State security) - i.e. the matters "in any case" excluded from the scope of the Directive - the "***specific national and international legal rules***" governing such matters override any contrary provisions in the data protection law. However, otherwise that law applies, and of course the constitutional imperatives, noted above, including the principles of *accessibility*, *foreseeability*, *necessity* and *proportionality*, also continue to apply to such processing.

On paper, it looks as if the data protection law in Sweden is given a ***very low status***: according to Section 2 of the law, **any legal provision in any other law decided by parliament or the government**, ***overrides*** the requirements of the general data protection law. However, this is the result of a a general constitutional approach rather than indicative of any low regard for data protection. Specifically, in Sweden it is felt that it should be up to Parliament to strike the balance between data protection and other interests when in comes to extensive personal data files with a sensitive content held by authorities. The general data protection law adopts an omnibus approach to data protection and does not contain exemptions for matters outside the scope of EC law or even a general provision equivalent to Article 13.1 of the Directive. The provision on subsidiarity in Section 2 of the general data protection law must be seen in this context. The omnibus approach ensures that any deviation from the provisions of this law is subject to a formal legislative procedure involving the government and, in many cases, parliament. During this procedure the Swedish data protection authority is heard and the compatibility with the Directive is scrutinised. Furthermore, the omnibus approach ensures that there is no gap in the protection afforded to individuals even in areas outside the scope of EC law.

Sweden has in fact gone out of its way to **review** all other laws and regulations relevant to data processing to ensure that they too complied with the Directive. This work (which took place between 1998 and 2001) by some counts covered some 30-odd laws, a dozen or so regulations, and less important provisions in a further 25 or so laws or regulations (although it is difficult to give precise numbers). The review resulted in new special data protection laws and regulations in areas where there were previously no data protection rules.

In the UK - which has no written constitution and no history of entrenched fundamental rights, even if the European Convention on Human Rights has now been (imperfectly) incorporated into the domestic system - the data protection law not only contains some very **wide exceptions** concerning processing based on other laws, but also ***gives way to any more specific or subsequent legal provision***; and the data protection law itself stipulates that information which is **obtained** from a person who is "***authorised by or under any enactment [law]***" must always be "***treateded as obtained fairly***" (as well, of course, as "**lawful**").

In sum, in countries such as Austria, France, Germany, Portugal, Spain and others, the very fact that data protection is constitutionally protected imposes important legislative constraints which, in effect, will ensure that all laws and lower legal regulations touching on this matter will be (or at least should be) read and applied in accordance with the Constitution - and thus (broadly speaking) with the Directive.[21] However, in other Member States this is less certain. It would therefore seem advisable (also in view of the constitutional anchoring of data protection in the Charter) to require the Member States to adopt a rule on the lines of the Greek or Danish laws, according to which the laws which give effect to the Directive prevail over other national laws in matters of data protection, at least as concerns processing relating to activities within the scope of Community law.

- o – O – o -

[21] In Germany, the Constitutional Court allows the legislator some time to rectify such shortcomings - but in rare cases, the legislator finds it impossible to do so within a reasonable time. Given the generally very high regard given to data protection in Germany, it is therefore somewhat ironic that one example of such a delay is the non-adoption of specific data protection rules for the Federal Criminal Investigation Office (BKA) in spite of a Constitutional Court judgment years ago that the Constitution required the adoption of such special rules. But that is the exception that proves the rule.

4. transnational issues (i) - "applicable law" [Art. 4]

introduction

Since the main purpose of the Directive is to ensure the smooth operation of the Internal Market, transnational matters are of particular importance. The Directive therefore, first of all, tries to ensure that there are no (positive or negative) **conflicts** between the laws of the Member States, i.e. that to any one processing operation falling within the scope of the Directive one law of a Member State applies, and not more than one law (or no law). Secondly, the main provision in the Directive (from the point of view of the Internal Market) is the stipulation, in Art. 1(2), that the Member States shall "neither restrict nor prohibit" the **free flow of data** between them for reasons of data protection (the other stipulation in Art. 1 of the Directive, to the effect that the Member States must ensure a high level of data protection by implementing the Directive, is in a way merely the *conditio sine qua non* for the creation of the "free zone" for data transfers announced in the second paragraph). And thirdly, the Directive tries to harmonise the Member States' approach to **transfers of personal data** from their territories (i.e. from the territory of the Community) ***to other*** (so-called ***"third"***) ***countries***. This section examines the first issue: the question of "applicable law" (after briefly looking at a more general, preliminary issue: the status of the non-EU EEA States); the other issues are addressed below, at 14.

summary of findings

The study found that there are still **substantial differences** between the "applicable law" provisions in the laws of the Member States. As a result, ***positive and negative conflicts of law remain*** between the Member States

One aspect of this is that - in this respect and in respect of cross-border transfers - some Member States treat the **non-EU EEA States** (*Iceland*, *Liechtenstein* and *Norway*) as (or on a par with) the EU Member States, while others regard them as "third countries".

There are also **serious problems** with the implementation of the first main rule in the Directive, that "*each Member State shall apply [their national law] to the processing of personal data where ... the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*". This rule is not fully or properly - and especially not consistently - applied in all the Member States, which results in the very kinds of conflicts that Art. 4 of the Directive seeks to avoid. Partly, this is the result of

deficient transposition of the Art. 4 of the Directive; but partly, it is caused by the **excessive complexity of that provision itself**.

In addition, ***the uncritical application of the "applicable law" provision in the Directive, without distinction between matters within and without the scope of Community law***, can (indeed will) result in the laws of Member States not applying to processing in their own country (or of data on their own citizens), on the assumption that the processing will be subject to the law of another EU Member State which provides "equivalent" (or at the very least "adequate") protection - when in fact, if such a foreign law applies, it may, in respect of matters outside the scope of Community law, provide **no such protection at all**. This could raise **serious constitutional issues** in the Member States and the Union.

matters to be further clarified or addressed

The question of whether - in view of the fact that the Directive has been added to the *acquis* of the EEA - the **non-EU EEA States** should be treated as EU Member States, or whether they should be treates as "third countries" will be clarified by the Legal Service of the Commission.

The "**applicable law**"-rules in the Directive will need to be ***re-drafted*** in such a way as to ***remove ambiguities*** in the present text, and will then have to be ***implemented identically*** in the Member States, if one of the main purposes of the Directive is not to be defeated. If the Directive were to adopt unambiguously the "***country-of-origin***" approach usually adopted for Internal Market measures, certain ***compensatory*** stipulations may be required (which could be modelled on corresponding provisions in other Internal Market Directives, such as the *e*-Commerce Directive).

- o – O – o -

4. transnational issues – detailed findings

4.1 EU\EEA and third countries

Article 4 of the Directive, which determines the law which is "applicable" to any particular processing operation (as discussed below, at 4.2), refers to controllers established in a "**Member States**" and to controllers who are not established on "**Community territory**", i.e. who are established in a State which is not a Member of the European Community. The latter States are called "***third countries***" in the other main provision dealing with transnational issues, Art. 25, discussed below, at 14. These concepts are important because "Member States" are treated differently from "third countries" in both respects: as concerns the question of "applicable law" and as concerns international data transfers.

However, three States - Iceland, Norway and Liechtenstein - have entered into an agreement with the EU called the "**European Economic Area**" or **EEA** under which they can agree to implement EC law in certain areas. The EC legal matters concerned are regarded as the "***acquis***" of the EEA, just like matters covered by EC legislation are referred to as the "***acquis***" of the EC. The Directive has been added to the "acquis" of the EEA. This means that the three non-EC EEA countries just mentioned must implement the Directive, just like the EC Member States must.

This raises the question of whether these States should be regarded as "Member States" (or treated as such) or whether (in spite of having to implement the Directive) they remain "third countries". This question is not the same as the question (raised in connection with transborder data flows, as discussed below, at 14.3) of whether the law in the non-EU EEA countries provide "**adequate protection**". By implementing the Directive, they clearly do. The problem is that "third countries" which provide an "adequate" level of data protection are still not treated in the Directive as "Member States" - also not as concerns the question of "applicable law", discussed below, at 4.2.

The point is that, as far as the issue of "applicable law" is concerned, the non-EU EEA States are treated as ***EU Member States*** in the laws of Germany, Ireland,[22] Sweden and the UK - but as "***third countries***" by the laws in the other Member States and in the proposed new (amended) law in France.

The Commission has agreed to ask the Legal Service for clarification on what is the correct legal approach in this respect. Pending this advice, it must suffice to note that the EU Member States which have implemented the Directive do not agree on this matter, and that the laws accordingly show **divergencies** in this regard which must be removed in the context of the revision of the Directive.

[22] In Ireland, this legal situation was reached as a result of a Statutory Instrument, the European Communities (Data Protection) Regulations 2001, which came into effect in May 2002 and which amended the Data Protection Act 1988 on the basis of the European Communities Act 1972. The relevant provision is repeated in the same terms in the Data Protection (Amendments) Bill which will (when adopted) bring other aspects of the law in line with the Directive.

4.2 **territorial scope of the Law** (the question of "applicable law")

> "1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
>
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;[23]
>
> (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
>
> 2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself."
>
> (Art. 4 of the Directive)

Article 4 of the Directive is, in some ways, the **cornerstone** of the data protection edifice erected by that instrument. If applied fully consistently by all the Member States it will avoid both conflicts of law between them and gaps in protection (in the sense of no law applying to certain processing operations). That was - and is - its purpose. If this can be achieved, a certain, limited measure of divergencies between the substance of the laws of the Member States is even acceptable. Yet unfortunately, it is phrased in such **complex terms** that it almost invites different (divergent) applications.[24] The national provisions implementing this article therefore require particularly close scrutiny.[25]

The first main rule in Art. 4 is that the Member States must apply their national laws to processing which is "**carried out in the context of the activities of an establishment of the controller on the territory of the Member State**". The laws in eight of the Member States

---

[23] The implementation of this provision (which concerns places such as embassies or ships flying the national flag) is not as such further examined here (except for one reference later in the text, relating to the Luxembourg law, for reasons explained there). It may suffice to note that some Member States repeat this stipulation, while others do not because (in their legal systems) the point is obvious.

[24] See my detailed analysis of this provision (with reference to its drafting history) in section 3.iv. of the FEDMA\DMA-USA publication Report on the Directives (with further references).

[25] Other matters (such as credit, or consumer protection, or environmental matters, or advertising, or indeed criminal matters) may be subject to the law of the country where goods or services are offered or bought, or where the consumer is based. Such "patchworks" - in which different aspects of a consumer-company relationship are subject to laws from different Member States - pose problems for companies and consumers alike, in particular also in the context of *e*-commerce. It would therefore be desirable to try and bring the "applicable law" provision in the Data Protection Directive in line with corresponding provisions in other Directives (including those relating to *e*-commerce). The matter is beyond the scope of this comparative study, but should be addressed in the context of the revision of the Directive.

(Belgium, Finland, Greece, Ireland,[26] the Netherlands, Portugal, Sweden and the UK) follow the text of this stipulation closely, although not always exactly.[27] One (Austria) elaborates on the matter in different terms than the Directive, but in a very helpful way; while four (Denmark, Germany, Italy and Spain) apply their laws differently from the way envisaged in the Directive. The law in Luxembourg is ambiguous.

The laws in the Netherlands and Portugal use the exact phrase from the Directive, quoted above in bold, *verbatim*; and the law in Belgium too uses these same words (with clarification as to what constitutes "establishment", but that too is taken from the Directive: see the 19th Preamble). The UK and the Irish law[28] are somewhat verbiose in that they stipulate that they apply to a data controller "in respect of any data" (UK) or "in respect of the processing of personal data" (Ireland), "***if the controller is established in [the United Kingdom\the State, i.e. the Republic of Ireland] and the data are processed in the context of that establishment***". In spite of a somewhat confusing stipulation about when a person or company is to be "***treated as established in***" the UK or the Republic of Ireland in this sense, these laws still pretty much faithfully applies the first rule in the Directive (and can certainly be read in that way). The proposed new (amended) law in France stipulates that it applies to "processing of personal data ... ***the controller of which is established on French territory***", while making clear that this should be read, in accordance with the Directive, as referring to ***processing taking place "in the context of" an establishment of the controller on that territory***.[29]

The law in Finland refers to "processing of personal data ***where the controller's establishment is situated on the territory of Finland***"; the Greek law to "***processing by a controller established on the territory of Greece***"; and the Swedish law to "***controllers of personal data who are established in Sweden***" - i.e. none of these refer to the processing having to take place "*in the context of the activities of*" the establishment of the controller in question, but these phrases can, and should, be read in line with the Directive.[30] The Luxembourg law says that 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 in a place where Luxembourg law applies by virtue of international public law (such as embassies) - but the ambiguity in this crucial context is not helpful.

None of these 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***

---

[26] In Ireland, this is again the result of the statutory instrument which came into effect in May 2002: see footnote 15, above.

[27] The Portugese law contains a somewhat different rule on "applicable law" with regard to "***video surveillance and other forms of capture, processing and dissemination of [identifiable sound and image data]***", which is further discussed below, at 10.4. By contrast - as already noted above, at 2.1 - the Luxembourg law expressly stipulates that its provisions apply, without modification, to the processing of such data; and this of course includes its rules on "applicable law".

[28] As amended by the statutory instrument mentioned: see footnote 15, above.

[29] The law refers to an "arrangement" (*une installation*) without adding that this arrangement must be a "stable" one (see the 19th Preamble to the Directive), but the term is likely to be read in accordance with the Directive and European law generally.

[30] In the Explanatory Memorandum to the draft of the Swedish data protection law it was noted that Article 4 of the Directive is unclear and that clarifications require international cooperation. Furthermore, it was expressly stated that the provision on territorial scope in the law should be interpreted the same way as Article 4 in the Directive. See Legislative Proposal 1997/98:44 pp. 55 and 118.

controller in another EU 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 the activities of an establishment of that controller in another EU Member State*** - although that is what the Directive intends. However, the non-applicability of the 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 Explanatory Memorandum to the Belgian law even usefully adds that, in the latter case, the Belgian-based controller does retain the obligation (under the Belgian Law!) to ensure that all its establishments (branches, wholly-owned subsidiaries etc.) comply with the law of the other (EU) state in which they are based in any processing of personal data carried out "in the context of" those establishments. This correctly explains the requirement set out in the second part of Art. 4(1)(a) of the Directive, that "*when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable*".

As far as Ireland, Sweden and the UK are concerned, this rule extends to processing in the context of the activities of an establishment of a controller in ***any of the non-EU EEA States*** (Iceland, Liechtenstein and Norway), because these are treated like the EU Member States in the laws of these countries (as was noted above, at 4.1).

More problematic is the fact that in the application of these rules, the laws in the above-mentioned countries do not ***distinguish*** between **matters within and without the scope of Community law** (or the Directive) (see above, at 3.3). This means that these laws also do not apply to processing which takes place in the context of the activities of a controller in another EU (and as far as Ireland, Sweden and the UK are concerned, EEA) State - even if the activities in question are outside the scope of the Directive. Thus, for instance, the collecting of personal data in the Netherlands or the Republic of Ireland in the context of the activities of (say) the British security services would not be subject to the Dutch or Irish law, but to the UK one (which in that respects provides much less protection and may indeed fall short of Dutch and Irish constitutional requirements). This is a problem which these Member States do not appear to have recognised.

The Austrian law is particularly interesting in this respect. The relevant provisions do not follow the precise text of the Directive, but in some ways make the intention of the Directive clearer than the Directive itself; and they do address the above-mentioned issue. Leaving aside certain complications deriving from a rather complex set of terms relating to "processing",[31] the law stipulates, first of all, 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**" (and from the other main rule, concerning non-EU-based controllers, discussed below) are "permissible only in ***matters outside the scope of***

[31] See section 2.2. I have used the term "processing" in the text in this section where the official German text uses "***Verwendung***", which is translated in the English translation of the Austrian law published by the Austrian Data Protection Authority by the word "use".

Community law".[32] The latter is a (limited) recognition of the fact that the main rule in Art. 4(1) of the Directive (like the Directive as a whole) 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 at least allows for corrective measures if the application of this rule leads to data subjects being deprived of adequate (or indeed possible all) data protection in particularly sensitive matters (such as "Third Pillar" matters).

By contrast, the laws in Denmark, Germany, Italy and Spain all contain provisions on their territorial application which in some respects **differ from the main rule 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 (say) the USA. 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.[33]

In recognition of the fact that adequate data protection is not ensured by the Directive with regard to matters outside its scope (as discussed above), 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. (broadly speaking) if the processing relates to ***matters outside the scope of Community law*** (such as, in particular, "Third Pillar" activities). It follows (both *a contrario* and because that is what the Directive intends) 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 disinguishes 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 (in whole or in part?) ***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**. Presumably, the law applies (at least in principle) to processing by a controller based in Germany, even if the processing (or part of the processing) takes place abroad. But what if the processing (or a part of the processing) is carried out in another EU\EEA State by an establishment of the German controller in that other EU\EEA State?[34] If one applies the second rule *mutatis mutandis* (as should be done according to the Directive), it should be the law of that other EU\EEA State that applies and not the German law - but the law is silent on this.

---

[32] D: *Angelegenheiten ... die nicht dem Recht der* ***Europäischen Gemeinschaften*** *unterliegen*. The English translation, referred to in the previous footnote wrongly uses the words "European Union" here - which misses the crucial point.

[33] I was informed by the Danish Justice Ministry that according to the Danish version of the Directive the law should only apply to activities carried out in Denmark (and not within the territory of the EC). The committee which discussed how to implement the Directive in Denmark found that it was not the purpose of the Directive to have such a limited scope. After some consideration the committee found that Art. 4 of the Directive should be interpreted in the way that the law should apply to activities carried out within the territory of the EC.

[34] The German law treats the non-EU EEA States on a par with the EU Member States: see above, at 4.1.

Secondly, there is the (not uncommon) situation in which an establishment in Germany of a controller from another EU\EEA State carries out what could be called purely technical processing on behalf of its parent company, i.e. this processing, although "carried out by an establishment (of the controller) in Germany", takes place, not "in the context of the activities of" that German establishment, but "in the context of the activities of" the parent company in another EU\EEA State. In terms of the Directive, this means that the "applicable law" should be the law of establishment of the parent company. The German law could be read as suggesting that that law applies, but can perhaps in this respect be interpreted in accordance with the Directive.

The Italian law applies to "***processing of personal data, by anyone,* carried out on the territory of [Italy]**";[35] and the Spanish law to "**processing [which] is carried out on Spanish territory *as part of the activities of an establishment of the controller***." In my opinion, neither of these rules properly reflects the first main rule in Art. 4(1)(a) of the Directive - but the Spanish data protection authority feels the text leaves scope for interpretation in line with the Spanish law.

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; but partly, it is caused by the **excessive complexity of that provision itself**.

Finally, I should recall that a further problem arises from the fact that the laws in Austria, Italy and Luxembourg apply to **legal persons**, while the others do not (although they may extend a measure of protection to such persons). As already noted above, at 3.2, the "applicable law"-provisions in the laws of the Member States result in these three national laws sometimes applying to controllers situated in another Member State; and conversely the law of those other Member States sometimes apply to controllers based in Austria, Italy or Luxembourg. In the first situation, controllers in such other countries then become subject to rules on the processing of data on legal persons which do not usually apply to them; while in the second situation, controllers in Austria, Italy and Luxembourg are not subject to such rules even though they usually do have to comply with them. Here, it must be added that both these situations are further complicated by the fact that Art. 4 of the Directive is not uniformly applied.

The second main rule in Art. 4 is that each Member States must apply its national law to processing where "**the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment** [or *means*: see text]**, automated or otherwise, situated on the territory of [that Member State]**." The Member States must also stipulate in their laws that such a controller must, in such a case, "designate a **representative** established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself." These rules are subject to an **exception**, in that the Member States must not apply their law in this situation if the "**equipment**" in question is "***used only for purposes of transit through the territory of the Community***."

---

[35] It: *la presente legge si applica al trattamento di dati personali da chiunque effettuato nel territorio dello Stato*. I have added the commas in my English translation to make clear that the words "on the territory of [Italy]" refer to the place where the processing takes place (is carried out, *e effettuato*), and not to the place where the person by whom the data are processed is situated.

These rules and requirements of the Directive are basically applied as stipulated above in most of the laws of the Member States which have implemented the Directive - Belgium, Denmark, Finland, Greece, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the UK – and will be applied in this way under the new (amended) laws in France and Ireland - but still with **some variations and extensions**.

First of all, it must be noted that most of the language versions of the Directive use a term which translates into English as "**means**" rather than "***equipment***" (F: *moyens*; I: *mezzi*; P: *meios*; Sp: *medios*). The laws in all the above-mentioned countries except for Ireland, Sweden and the UK consequently also use terms corresponding to "means".[36] "Means" would appear to be wider than "equipment", which suggests a physical apparatus. Thus, the French data protection authority considers that if a controller established outside the EU sends a **paper form** to a data subject in France, that form constitutes a "***means***" used to process data. The same applies if a controller who is established outside the EU, and who himself uses a server situated outside the EU, collects data from a data subject who accesses his website by means of a **PC** or **terminal** based in France: in that case, the PC or terminal constitutes the "means" used by the non-EU controller to obtain data. The same would apply to the collecting of data by **telephone**. As another data protection authority remarked: "*in effect, all processing involves 'means'*". This view may also explain why some countries do not contain any reference to "equipment" or "means" in their laws at all, as noted below.

Secondly, as discussed above, at 4.1, several of these countries (again) treat the **non-EU EEA States** (***Iceland***, ***Liechtenstein*** and ***Norway***) as EU Member States in this regard, while others do not. This is the case in Denmark, Ireland, Sweden and the UK. This means that these four countries do not apply the above rule (the second main rule in Art. 4) to controllers in ***Iceland***, ***Liechtenstein*** or ***Norway*** who use "equipment" on their territory, while the other ten (Austria, Belgium, France (under the new law), Finland, Germany, Greece, Italy, Luxembourg the Netherlands, Portugal and Spain) do apply this rule (or even wider-phrased rules, as discussed below) to those countries.[37] This is particularly notable with regard to Finland, which in the other transnational context (transborder data flows), discusssed below, at 14, *does* treat the non-EU EEA States as EU States (see section 14.1).

Thirdly, there is some confusion about the exception with regard to controllers who use equipment for "**transit**" only. The Directive stipulates that this exception must be applied (i.e. that the law of the country in question must not be applied) if such equipment is (or such means are) "used only for purposes of **transit through the territory of the [European] Community**." This same wording is indeed used in the Italian and Portugese laws, while the Luxembourg law and the proposed new (amended) French law refer to ***transit through [Luxembourg\French territory] or through [the territory] of another Member State of the European Union***, which amounts to the same thing. The Danish law also refers to transit through the EU - but in that case, the reference to the Union should be read as also including the non-EU EEA States because, for the purposes of the Danish law, these are treated as EU States (as noted above, at 4.1). The Swedish law applies the exception if the equipment "is only used to **transfer** information ***between a third country [i.e. a non-EEA country] and***

[36] The Danish law uses the term "*hjælpemidler*", which is somewhere between "means" and "equipment", while the Swedish law uses "*utrustning*", which is closer to "equipment".

[37] Note that the rules concerning non-EU-based controllers were only added to the Italian law in December 2001.

another such country." However, the laws in Belgium, Finland, Ireland and the UK only refer to **transit *through the Member State in question*** (i.e. through Belgium, Finland, Ireland or the UK respectively). The laws in Greece, the Netherlands and Spain merely refer to "**transit**" without clarifying whether this means transit through their territory or transit through the EU. From the domestic point of view, the first interpretation would appear more logical, but if these laws are to be applied in accordance with the Directive, they should be given the second reading. Again, there is as yet **no clarification** of these matters in the practice of the national authorities.

Some of the Member States in fact apply their law to non-EU (or non-EEA) controllers **more widely than as suggested by the Directive**, or apply ***specific formalities more widely***. Thus (perhaps for the reason mentioned above), the Austrian and German laws apply to **all processing in**, respectively, Austria and Germany by a ***controller who is not established in the EU*** (or in the case of Germany, in the ***EEA***) - irrespective of whether the controller uses "***equipment***" (or "***means***") in their country. This includes, in particular, the ***collecting***" of such data in these countries, without the use of "***equipment***" or "***means***". The Danish law also applies to ***a controller who is established in a non-EEA country***, if "the **collection of data in Denmark** takes place for the purpose of processing in a [non-EEA] country" - again, even if no "***equipment***" or "***means***" are used in this. The repercussions noted in respect of a wide concept of "means", noted above, in particular as concerns the collecting of data by **mail**, by **'phone**, or indeed over the **Internet**, of course apply *a fortiori* in these cases.

The Austrian and Greek laws also extend the requirement that certain controllers must appoint a "**representative**" in their country beyond the situation envisaged in the Directive. The Austrian law requires the appointment of a representative by any controller whose **processing is subject to the Austrian law** (as discussed above, with reference to the rules in the Directive) but who is ***not established in Austria***; while the Greek law requires all controllers ***outside Greece*** to appoint a representative if they **process data on Greek residents**. It must be stressed that these provisions apply also to controllers in the other EU Member States. Whether that is compatible with the Directive is perhaps doubtful in that they could be seen as "**restrictions**" (in the form of a "***formality***") affecting the free flow of personal data between the EU Member States, in contravention of the fundamental principle establishing a "free zone" for intra-EU data transfers, stipulated in Art. 1(2) of the Directive and further discussed below, at 14.2. The provision is also problematic in relation to activities on the **Internet**, as discussed below.

Here, it must be noted first of all that there is, as yet, **no complete uniformity** in the application of the "applicable law" provision in the Directive. There are still **substantial divergencies** between the laws of the Member States. As a result, ***positive and negative conflicts of law remain*** between the Member States; and the treatment of ***non-EU (EEA) based controllers differs***.

Some of these problems can be resolved if the **EU\EEA issue** is clarified (see above, at 4.1) and if the laws that refer to "**transit**" through their own territory only are amended so that they refer to transit through the EU (as is required by the Directive). Some Member States however feel that a more fundamental review of the rules is in order, in particular as concerns the application of the law to non-EU controllers. As the UK Information Commissioner (the data protection authority) says:

> "It is hard to see the justification for applying the Directive to situations where a data controller is not established in any Member State but nevertheless uses equipment in a Member State for processing. If, for example, a business in the US collects personal information on US citizens in the US but processes the personal data on a server in the UK it is subject to the requirements of the Directive. This extra-territorial application of the law makes little sense, is very difficult if not impossible to enforce and is a disincentive for businesses to locate their processing operations in the EU. If a collection of personal data is controlled and used in a non-EU jurisdiction regulation should be a matter for that jurisdiction regardless of where the data are actually processed. Furthermore the Directive requires that a data controller outside the EU appoints a representative in the Member State where processing takes place. What is the purpose of this? There is no apparent basis on which the Commissioner could take action against a representative for a breach of UK law by a data controller established outside the EU."

A matter of particular difficulty is the application of data protection law (or indeed, any law) to the **Internet**. Article 4 of the Directive is again ***not easy to apply*** in that respect. The discussions of the Working Party have tended to focus on ***how*** to apply the (substantive) requirements of the Directive to activities on the Internet;[38] the primary issue of ***when*** these requirements (or rather, the requirements of the national laws of the Member States implementing these requirements) apply to a particular controller's activities on the Internet has been somewhat ignored. I have discussed the issue in some detail in my Report on the Directives, written for FEDMA and the DMA-USA: a copy of the relevant section (section 11.iv) is attached.

The matter has been similarly dealt with at the national level: while many data protection authorities in the Member States have provided guidance to controllers on ***how*** to comply with their law in their activities on the 'Net, they have been somewhat silent on the question of ***when*** the law in question applies to these activities in the first place. This is mainly because such advice is primarily directed at **domestic companies or organisations** who become active on the 'Net. These are clearly "established on the territory" of the State concerned, and any processing of data on the Internet by them clearly takes place "in the context of [their] activities." Their own domestic data protection law thus clearly applies to their Internet activities - what they need is guidance on how (according to that law) to inform data subjects; when (according to that law) they need to obtain the consent of the data subject (e.g. for "cookies"); etc. Reports on the matters raised under the relevant domestic law have been prepared in several countries; the data protection authorities have also addressed the issues in these terms in ther Annual Report.[39]

There is also not too great a problem as concerns the activities on the Internet of **controllers in another EU Member State**: those activities will (as far as data protection is concerned) be subject to the law of the country in which the relevant "establishment" is based on which the Internet activities focus. If a German company deals with Austrian consumers (data

---

[38] For a briefing on the Opinions and Recommendations of the Working Party in this respect, see my paper, European Data Protection Law & the Internet, produced for FEDMA and PLI (the Privacy Leadership Initiative) in December 2000.

[39] See (e.g.) re Austria, the (unofficial) "FAQ" on how the Austrian law applies to the Internet published on the website of the data protection action group *Arge Daten*; the Danish report *Persondataloven geografiske anvendelsesområde* (November 26, 2001); the report by the Swedish Data Protection Authority, *Personuppgifter på Internet* (1999); or the chapters on the Internet in the latest Annual Reports (covering 2001) of the French and Italian Data Protection Authorities.

subjects) directly from its own base in Germany, the personal data processing involved will (or at least ought to be) subject to the German law, and not to the Austrian one, and *vica versa*. If this activity is carried out more-or-less independently by a separate Austrian office or branch, the Austrian law will apply. Etcetera.

A problem does arise however when it comes to the application (or not) of the law of a Member State to activities on the Internet by **non-EU** (or perhaps ***non-EEA***) **controllers**. As explained in the attached section from my FEDMA\DMA Report on the Directives, in terms of Art. 4 of the Directive the crucial issue is whether the obtaining of data by such controllers on "visitors" to their websites (e.g., through "cookies") involves the use of "equipment" in the country where the "visitor" is based (there is little doubt that data are transferred across borders, but that is a different question, addressed below, at 14.3). This is also true of the laws in the Member States which basically follow the text of the Directive in this respect, without extending the law beyond what is suggested there. The data protection authorities are understandably reluctant to extend the application of their national laws to situations in which they cannot effectively enforce them, and especially so if data protection is in a way only marginal to the issue raised.

> EXAMPLE: The Portugese data protection authority refused to act on a complaint brought by Portugese pharmacists about the selling over the Internet, by companies based in the USA, of medicines which required a prescription in Portugal. They ruled that in that case the Portugese data protection law did not apply.

However, as was also noted above, the laws of Austria, Denmark, Germany and Greece are all extended in such a way that they also apply to the ***collecting*** of data in the country when no "***equipment***" is used (in Greece if this involves collecting data on Greek residents); and the laws in some other Member States apply the term "***means***" (used rather than "*equipment*") very broadly. It would appear that the obtaining of data on "visitors" from such countries by webhosts outside the EU\EEA (e.g., in the USA) is thus subject to the law in those countries. This of course brings with it a host of responsibilities for the controllers concerned - including the duty to appoint a "**representative**" in each of them; duties to inform the data subjects; notification; etc. etc. The Danish data protection authority has in ***some cases*** applied the special rule concerning the collection of data in Denmark when no equipment is used, and has had ***only minor problems concerning enforcement***. The French data protection authority feels that the right to enforce the law (i.e. to claim that the law applies according to the rules discussed in this section) should not be surrendered, and indeed that criminal penalties may be applied if necessary, in accordance with the general principle that French law can be enforced against actions the ***effect*** of which are felt in France. But at the same time, the authority recognises that the formal requirement that a "***representative***" be appointed can perhaps be dispensed with, since it is "unrealistic" to expect non-EU controllers to comply with it. The authority has pointed out its action against the US webhost *Yahoo!* and others.

However, in the other Member States, there is little evidence of serious attempts to enforce the laws *vis-à-vis* non-EU\EEA controllers. As the Irish data protection Commissioner put it: "*we should not pretend to control what we cannot in fact control*."

ATTACHED**:** Extract from D Korff Report on the Directives, FEDMA\DMA-USA, 2002

- o – O – o -

ATTACHMENT TO SECTION 4.2 (the question of "applicable law":

Extract from D Korff, Report on the Directives, FEDMA\DMA-USA, 2002:

(d) applying the rules on "applicable law" to the Internet

The Working Party is of course right in its opinion (quoted above, at (b)) that "the Internet is not a legal vacuum", and that, as it put it elsewhere:

> "... activity on the Internet cannot be exempted from the basic legal principles that are applied elsewhere. The Internet is not an anarchic ghetto where society's rules do not apply."[40]

However in practice, applying law - and not just data protection law - to the Internet is highly problematic.[41] Even so, before looking at possible "pragmatic" solutions (see below, at (e)), we ought to first examine the legal rules on "applicable law" - especially because in many EU Member States - and indeed, as explained above, at 1.*iii*, in the Union) - data protection is a matter of (constitutional) "*ordre public*" which cannot be simply set aside or "pragmatically" reduced. As long as there remain differences in substance between the national laws of the Member States - as there will be, even after the Directives are fully implemented - the rules determining which law is applicable therefore remain crucial.

As explained above, at 3.*iv*, the Directive seeks to ensure, by means of its provision on "applicable law" (Art. 4), that the laws of the Member States adopted or amended in order to give effect to the Directives (both the framework Directive and the subsidiary Directive) do so without either causing conflicts of law or situations in which none of the national laws applies. The question of which of these national laws applies to a particular processing operation in cyberspace should therefore be determined by reference to this article.[42]

According to this article, once it has been established that "personal data" are being processed on the Internet (as discussed above, at (b)), one has to clarify: (1) who the *controller* of the operation is; (2) what "*establishments*" of this controller are involved in the operation and where they are based; and (if any of these establishments are situated in the EU\EEA) (3) in the *context* of the activities of which of these establishments the processing can be said to be taking place. If the controller is not "established" in the EU\EEA, one has to ask (4) whether the controller makes use of any "*equipment*" in the EU\EEA for the purpose of the operation. Let us examine these issues step by step.

The first question is: who is the controller of the processing, i.e. who determines the purposes and means of the processing (e.g. who decides what to do with traffic or

---

[40] WP 06, p. 6.

[41] The Working Party noted as matters in need of regulation, with reference to various Green Papers, Commission Communications, Council Resolutions and legislative initiatives: child pornography; the use of the Internet for communications in support of "off-line" criminal activity; taxation (particularly VAT) of on-line commercial activity; and the protection of intellectual property rights in respect of content distributed on-line (see WP 06, p. 3). For illustrations of contentious applications of some countries' criminal law (and civil law of defamation) to Internet websites see, e.g. "Sex online 'is prostitution'", Guardian, 16 February 2000; "Gay teacher takes on 'evil' website", Guardian, 12 April 2000; "Libel threats blight websites", Guardian, 15 April 2000; "Yahoo! faces French fines for Nazi auctions", Guardian, 24 July 2000; "French seek way to bar Yahoo site", Guardian, 12 August 2000. The question raised in all these contexts is when one country's law should be applied to a website hosted by a company or organisation based elsewhere. To do so merely because the website can be accessed from a country clearly raises serious problems.

[42] Note that the question of "applicable law" may be more confused in practice, if the Member States fail to implement Art. 4 in the same way: see above, at 3.*iv*.

"clickstream" data, or whether to use "cookies" and how to use the data captured)? With regard to processing for routing and connection purposes etc., this will normally be the ISP; with regard to the use of "cookies" this will be the website host (the identity of that controller may not always be immediately obvious to the user - but that merely underlines the need to clarify the identity of the controller in a given context to the user, e.g. on a website: see above, at 4.*iii*(a)).

We must then determine whether the controller is "established" in the EU, i.e. whether the company in question has an office or branch or subsidiary in an EU\EEA State. If this is the case, the law of that State will apply to the extent that the processing of the personal data can be said to be taking place "in the context of the activities of" that establishment in the EU\EEA. As it is put by the Working Party:

> "... businesses, organisations and individuals established within the EU and providing services over the Internet will ... be required to follow the rules established in the data protection directive 95/46/EC (as implemented in national law) as regards any personal data that they collect and process [read: in the context of the provision of those services]."[43]

Clearly, personal data processed by an EU\EEA-based ISP, or by an EU\EEA-based company through its own website, is thus subject to the law of the EU\EEA State in which the ISP or company is established (with regard to the company, this is irrespective of whether the company has a .com site or a .co.uk or .co.de or whatever site). Indeed, the Working Party has stressed that such controllers should not try to seek the agreement of its subscribers to arrangements which fall short of the European rules - as the Working Party believes P3P has tried to do:

> "There is a risk that P3P, once implemented in the next generation of browsing software, could mislead EU-based operators into believing that they can be discharged of certain of their legal obligations (e.g. granting individual users a right of access to their data) if the individual user consents to this as part of the on-line negotiation. **In fact those businesses, organisations and individuals established within the EU and providing services over the Internet will in any case be required to follow the rules established in the data protection directive 95/46/EC (as implemented in national law) as regards any personal data that they collect and process.** P3P might thus cause confusion not only among operators as to their obligations, but also among Internet users as to the nature of their data protection rights. Browsing software that is sold or distributed within the EU must therefore be designed and configured so as to ensure that on-line agreements which are in contradiction with prevailing data protection laws are not possible."[44]

If a company has different branches or subsidiary companies in different EU\EEA countries, and if each of these hosts its own independent website, the data protection law applicable to each site would be the law of establishment of the branch or subsidiary company that runs that site. If a company targets its site, not on a national but on (say) a linguistic basis, the applicable data protection law will remain the law of the country where the company or branch responsible for the particular language site is based. Thus, for instance, a German company may have a German-language .co.de site, aimed at (potential) customers in Germany, Austria, Switzerland and Luxembourg. On the basis of Art. 4 of the Directive, all

---

[43] WP 11, p. 1.

[44] Opinion 1/98 on the Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), WP 11, pp. 2 – 3, emphasis added.

the processing of personal data on that site must be subject (only) to German data protection law - and not to the Austrian or Luxembourg law (whether Swiss law applies would depend on whether Switzerland had adopted a rule similar to Art. 4 of the Directive, but while Austria and Luxembourg are required to do so, Switzerland as a non-EU\EEA State is not).[45] But if the site was hosted by an Austrian company, or a Luxembourg one, the applicable law would be (only) the Austrian, respectively Luxembourg, data protection law.

If a non-EU\EEA-based company establishes a separate website for its European customers, registered by reference to a country in the EU\EEA in which it has an establishment, that suggests strongly that the processing of the data by means of this website takes place in the context of the company's European operations. Thus, for instance, if a US corporation sets up a separate website under corporation-name.co.uk (or .co.de or .co.fr or whatever), to which it directs its UK (or more generally its European) customers, and which is effectively run by its EU\EEA establishment (or establishments), then the US corporation can convincingly argue that the data captured there are processed "in the context of the activities of" its UK (or German, or whatever) establishment(s) - even if it (the US mother company) were to remain the controller. This would apply *a fortiori* if the European subsidiary or branch set up the website autonomously, independently from its US head office (although in that case the European subsidiary rather than the US mother company would be regarded as the controller).[46]

In all these circumstances, there is an EU\EEA-based controller of the processing of the data on the 'Net, and consequently the applicable data protection law is the data protection law of the country of establishment of that controller: see above, at 3.*iv*(a).

If an (e.g.) US-based ISP or other (tele)communications service provider, or any other kind of US-based company which is not "established" on EU territory (i.e. which does not have an "establishment" in an EU\EEA State) but which hosts a .com website that can be accessed from the EU\EEA, captures personal data on European users of its services, or on European visitors to its website, the question arises whether the US company can be said to be "making use" of "equipment" "situated on the territory of" an EU\EEA State to carry out this processing. If it does, the law of any country in which such "equipment" is situated will apply, unless the equipment is only used "for purposes of transit through the territory of the Community [the EU\EEA]": see above, at 3.*iv*(b).[47]

The US corporation's visitors use their PCs to access the .com site but it is a bit far-fetched to say that the US corporation "makes use" of its visitors' PCs to capture their data. One could argue - as Poullet *et al.* do[48] - that when an individual accesses a website:

> "there is simply a transfer [read: of that person's personal data, by that person] to a third country".[49]

---

[45] Note that the Commission decisions on the "adequacy" of the data protection laws of third countries - i.e. until now, of the laws in Hungary and Switzerland - discussed above, at 10.*iii*(b), do not address this question.

[46] The question of who is the controller has important implications on *how* the national law in question must be applied, as will have become clear from the other sections in this report. This section is only concerned with the question of *whether* a national law of an EU\EEA State applies to a website, and on what that depends.

[47] The same applies if the US corporation does have an EU\EEA establishment but this EU\EEA establishment is not involved in this particular activity (i.e. the data are not processed in the context of the activity of the EU\EEA establishment): see footnote 51, *supra*. Note that if a law of an EU\EEA country applies on the basis discussed in the text, the non-EU\EEA controller must designate a "representative" in the country concerned: Art. 4(2) of the Directive. In practice, since websites can be accessed from any country, this would mean that the controller would have to appoint representatives in all EU\EEA Member States.

[48] Poullet *et al.*, o.c. (*supra*, footnote 186), p. 57, footnote3, with reference to other authors.

In fact, the situation is not so simple. In particular, the issue of whether there is a (cross-border) transfer of data in a particular context has little relevance for the question of whether any European data protection law - or laws - applies (or apply) to the processing. The rules on data transfers are contained in Arts. 25 and 26 of the Directive, as discussed above, at 10. But the question of "applicable law" still has to be answered on the basis of Art. 4.

It is difficult to deny that ISPs, or corporations hosting websites, "makes use of" pipes and networks and servers (i.e. of "equipment") to enable use of their services, and\or to create a presence on the 'Net; and it would be unreal to argue that the relevant activities of the corporation are not (also) "for purposes of processing personal data" - i.e. aimed at collecting and retaining data on users. Some of the pipes and some parts of the networks involved in allowing European visitors access to the network and to the .com site will be physically located in the EU\EEA; they will carry the data on the visitors which are captured by the ISP and the host. Strictly speaking, this “equipment” is not used only for the purpose of transit through EU\EEA territory: it is used to send data from the EU\EEA to the site and *vica versa*. As far as the website host is concerned, the server may (or may not) be situated in the EU; if it does, it too is “equipment” "used" by the host to receive and send data to and from the EU\EEA (i.e. not just in order to transit the EU\EEA). However, from a technical point of view, the location of a server is becoming less and less important as data transfers are increasingly directed to server farms which can be sited anywhere.

In practice, the situation is even more confused, in that:

> "... the allocation of responsibility for clickstream data may be difficult to discern. The clickstream data generated by on-line activities is initially processed by an Internet access or service provider. The bits and bytes are then shared with a myriad of parties to on-line service transactions. The localization of relevant processing activities may be quite variable." [50]

Yet in legal terms, these difficult-to-discern and in technical terms increasingly irrelevant aspects of data processing on the Internet would appear determinative of the applicable law, indeed may result in the simultaneous application of many (or indeed all) EU\EEA national laws to any one (non-EU) website.

The Working Party and the Commission are of course aware of the problem of applying Art. 4 of the framework Directive to the Internet, but (as with the question of whether certain data are "personal data") are reluctant to concede too much too quickly, for fear of European Internet users loosing all protection. Thus, the Working Party felt constrained to warn, in the context of its Opinion on the Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), that its comments on these (self-regulatory) proposals were:

> "... without prejudice to a more detailed examination of [the application of] Article 4 of directive 95/46/EC, which could be construed as rendering the directive applicable to third country websites collecting data from EU-based users."[51]

Tthe Commission decision on the "Safe Harbor" arrangements (discussed above, at 10.*iv*) similarly stresses that that decision:

---

[49] The English text has "transfer to a third *party* country" but it is clear from the context and the original French text of the study ("*transfert vers un pays tiers*") that this should read "transfer to a third country" in the sense of Art. 25 of the Directive.

[50] Reidenberg & Schwartz, o.c. (*supra*, footnote 271), p. 24.

[51] WP 11, containing Opinion 1/98 on P3P and OPS, footnote 1 on p. 3.

> "does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States, in particular Article 4 thereof."[52]

The Commission expressed the same sentiment even more forcefully in the letter with which it informed the US authorities of that decision:[53]

> **"Jurisdiction**
>
> During our dialogue, you raised with me the concerns of US industry about the possible effects of the 'safe harbor' as regards jurisdiction and applicable law in the European Union. I would like to confirm that it is the Commission's intention that participation in the 'safe harbor' does not change the status quo ante for any organisation with respect to jurisdiction, applicable law or liability in the European Union. Moreover, **our discussions with respect to the 'safe harbor' have not resolved nor prejudged the questions of jurisdiction or applicable law with respect to websites.** All existing rules, principles, conventions and treaties relating to international conflicts of law continue to apply and are not prejudiced in any way by the 'safe harbor' arrangement."

The problem is that faced with the threat of becoming subject to a multitude of ("approximated" but still divergent) laws of EU\EEA Member States, US and other non-EU\EEA corporations will be tempted to exploit loopholes to escape the EU data protection regime - such as, in particular, the possible exemption from that regime with regard to the processing of data which in some EU Member States at least are not regarded as "personal". As Reidenberg and Schwartz note:[54]

> "In terms of the Internal Market, the effort to provide an exclusive choice of law and the possibility that overlapping jurisdiction may still occur raise substantial incentives for developers of on-line services to try to circumvent particular data protection rules through infrastructure architecture. The on-line environment is geographically flexible. Controller's functions may be disaggregated and routed to take advantage of differences in the 'margin of manoeuvre' among the Member States. For example, a French on-line service provider may allocate dynamic IP addresses on equipment located in the United Kingdom to try to avoid the applicability of French data protection law for the recipients of those IP addresses. Under this scenario, United Kingdom law would apply to the IP addresses allocated by the British server and might result in the IP addresses falling outside the scope of data protection for the recipients of those addresses."

It is no doubt partly because of this that the Commission is looking for a special, "pragmatic" resolution to the problem, tailored to the needs and realities of the Internet, as discussed in sub-section (e).

---

52 Commission Decision on the Safe Harbor arrangements, *supra*, footnote 216.

53 Letter from Mr. John Mogg, Director-General of the Internal Market DG of the EC, to Mr. Robert LaRussa, Under-Secretary for International Trade of the US Department of Commerce, of 27 July 2000, DG Markt/E-1 D(2000)168, p. 3, emphasis added.

54 Reidenberg & Schwartz, o.c. (*supra*, footnote xxx), p. 140.

(e) the "pragmatic" approach

The Working Party's and the Commission's overall approach to the question of data protection and the Internet is two-fold. On the one hand, as explained above, at (a), they stress that the Internet is not exempt from the requirements of data protection but, on the contrary, that the basic data protection principles and –rules, as enshrined in the Directives, should be "fully" applied also to the collecting, dissemination and use of personal data on the Internet, including email addresses and traffic data. Similarly, as explained above, at (d), the Working Party and the Commission in their public pronouncements insist that the European rules enshrined in Art. 4 of the Directive ought to determine which is the "applicable law" with regard to any particular personal data processing operation - including processing operations on the Internet. They realise that there are practical and legal problems, but they emphatically reserve the right to resolve the legal questions in particular on their own terms.

On the other hand, the Working Party wants to be "pragmatic".[55] As we shall see below, at *ii*, it has looked in some detail at how the Directives' substantive requirements could or should be applied to the Internet. But it has refrained from suggesting that *all* the (highly detailed, technical and country-specific) requirements of *all* the national laws of *all* the Member States should *always* apply whenever this could theoretically be demanded (as discussed above, at (b) and (c)). As further discussed below, at *iii*, it has also (if less specifically) hinted at a regulatory and enforcement system (somewhat) detached from the regulatory and enforcement systems of the individual Member States.

Basically (and in my opinion rightly, if not unproblematically), the Working Party appears to be willing to accept, and to assist in the development of, special rules for the Internet, which - like the national laws of the Member States - are based on the requirements of the Directives, but without being tied to the national laws of the Member States. It has clearly decided to first focus on the substance of data protection on the Internet, on how to "translate" the requirements of the Directives into rules relevant and appropriate for that environment. It clearly hopes to persuade the main actors and regulators (including self-regulatory bodies), in the EU and elsewhere (and in particular in the US), to agree to those substantive requirements on terms as close as possible to the Directives - and there is the unspoken promise that, if adequate substantive rules are agreed and if adequate procedures and mechanisms are established to ensure that those substantive rules are properly implemented in practice, it will not seek to enforce the letter of each national law of each EU\EEA Member State. In return, the Working Party presumably hopes that non-European organisations and -actors on the Internet will accept those rules and submit themselves to such procedures and supervisory mechanisms, rather than challenge the right of the EU to impose its regime on the 'Net. The Commission appears to support this "pragmatic" approach.

The problem with this approach is two-fold. First of all, it will not be easy to reach an agreement on substance, or on supervision and enforcement, that both meets the minimum demands of the European authorities and is accepted by a sufficiently large number of non-EU (in particular, US) data controllers (ISPs and others).

Secondly, as things stand, the agreements reached may not withstand legal challenges in the EU\EEA Member States. Data subjects and controllers may argue, on the basis of different readings of terms like "personal data", or "public telecommunications [or: electronic communications] services", or "calls", either that certain specific national rules which are not fully reflected in the negotiated regime should be enforced *viz-à-viz* certain non-EU\EEA controllers in respect of their activities on the Internet; or conversely, that in law neither the

[55] Cf. the stress on this term in the last two paragraphs on p. 2 of WP 16.

national rules nor the negotiated regime applies to them. Both would invoke Art. 4 in support of their contention. Furthermore, the national data protection authorities may be unwilling, in specific cases, to forego the exercise of their jurisdiction (or they may even be legally incapable of so doing). In the end, the national courts in the Member States, and the European Court of Justice, would enforce their national law, and Art. 4 of the Directive as read by them, over and above any not-legally-binding agreement on data protection on the Internet. This applies *a fortiori* if the national rules and procedures in question are given strong constitutional protection - as is the case in several EU Member States (see above, at 1.*iii*)

The two issues are linked, in that the Working Party and the Commission are negotiating from a position in which they cannot accept a solution which would create serious constitutional problems in the EU or the Member States, and which could be subject to legal challenges at national constitutional- and European Court level, while non-EU controllers may not be queueing up to join an arrangement which commits them to adherence to - by world-wide standards, very high - minimum constitutional requirements of the EU and the EU Member States.

It will undoubtedly take long and difficult negotiations - similar to the protracted negotiations on the Safe Harbor but with the added complexity of a lack of a single government authority as the negotiating partner - to resolve these issues. In the meantime, all one can do is look at the recommendations and opinions of the Working Party for an idea of how the European authorities feel the data protection issues raised by the Internet ought to be resolved. This is done in the next sub-sections. In the end, however, any substantive and procedural matters resolved in these discussions may have to be confirmed in law - which may involve amending the Directives, or issuing "additional or specific measures" under the framework Directive, as provided for in Art. 30(1)(c) of that Directive. As explained above, at 1.*ii*, a review of the framework Directive is due in any case in 2001, and a proposal for a new Directive to replace the telecommunications data protection Directive is already under discussion. Arrangements of this kind should be proposed in the context of these reviews.

5. data quality (the data protection principles) [Art. 6]

introduction

The Directive lays down a number of principles which it calls "principles relating to data quality" but which in fact touch on wider matters. The study looked at the way in which the **principles** have been incorporated into the laws of the Member States ***generally***; at the crucial "***purpose-specification and –limitation principle***", and at the ***safeguards*** imposed in connection with (***secondary***) ***processing for research purposes***, for which the Directive provides an exemption.

summary of findings

The data protection principles are contained in the laws of all the Member States, with a few exceptions in terms identical to or close to those used in the Directive. However, **a few laws** use ***somewhat varying terms***; one sets out the data protection criteria (below, at 6) in the middle of the principles; and one adds ***further principles***. In addition, some countries add clarification or gloss to the principles, in ways which sometimes ***strengthen*** them but sometimes do the ***opposite***.

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. However, in spite of the similar wording, the very **vagueness** of the principle leaves it ***open to divergent application***, and different Member States apply **different tests** in this regard, ranging from the "***reasonable expectations***" of the data subject, to "***fairness***" or the application of various "***balance*" *tests***. In a few countries, the principle is subject to quite sweeping **exemptions** (in addition to the ones discussed at 10), in particular for ***public-sector controllers***.

The rules concerning secondary processing of personal data for research purposes without the consent of the data subjects, contained in the laws of the Member States examined so far, **vary very considerably**. Some fail to provide ***any safeguards*** (in manifest breach of the Directive); some lay down ***minimal*** (i.e. insufficient) ***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 academic "***ethics committee***", or require researchers to apply for a ***special authorisation*** from the Data Protection Authority, who is to stipulate various conditions (or these additional conditions may be spelled out in the law already).

Some laws apply their rather relaxed regime also to the use of **sensitive data** for such research purposes (in violation of the Directive), while others (rightly, and in accordance with the Directive) stipulate that the use of such data for such purposes may only be authorised if the research serves an "**important public interest**".

matters to be further clarified

The way in which the data protection principles have been transposed into the laws of the Member States illustrates extremely well how the mere repeating of the provisions of the Directive in itself does not ensure a harmonised application of the rules: the Member States give **highly divergent** guidance on how the principles are to be applied in practice and apply **quite different tests** in this respect. It shows the need for a ***mechanism*** under the Directive to provide ***central guidance, at the European level*** on such open-ended provisions.

The same applies with regard to the clarification of what are "**appropriate safeguards**" in terms of Art. 6(1)(e) of the Directive, concerning (secondary) processing of personal data for ***research purposes***. Again, the Member States (to the extent that they have provided such safeguards at all) have opted for **quite different kinds of safeguards**. While each of these can possibly ensure adequate protection, the very fact that they differ in nature and substance causes problems for cross-border research, and thus for the Internal Market.

- o – O – o -

5. data quality (the data protection principles) – detailed findings

5.1 general

> 1. Member States shall provide that personal data must be:
>
> (a) processed fairly and lawfully;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) kept in a form which 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. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
>
> 2. It shall be for the controller to ensure that paragraph 1 is complied with.
>
> (Art. 6 of the Directive)

The **data protection principles** (referred to as "***principles relating to data quality***" in the Directive) are set out in ***very similar*** (often even identical) terms in the laws of most of the Member States: Austria, Belgium, Denmark, Finland, Greece, Ireland,[56] Italy, Luxembourg, the Netherlands, Portugal, Sweden and the UK. They are also included in largely identical terms in the proposed new (amended) law in France. To the extent that there are variations in wording these are minor (e.g., the law in Denmark refers to "good practice" rather than "fairness").

The Spanish law literally prohibits the **collecting** of [personal] data by "***fraudulent, unfair or illicit means***" (SP: *medios fraudulentos, desleales or illicitos*) - but in practice this prohibition is extended to other forms of processing too, in accordance with the Directive. Indeed, the law adds particularly strict rules on other matters such as the up-dating of data, and the need to destroy data when they are no longer needed, which go beyond the rather general stipulations in Art. 6 of the Directive. There are more substantial differences between the Directive and the German law, as shown below, at 5.2 and 5.3, and that law also **adds some more principles**, i.e. that data must if possible be ***collected from data subjects***, and must generally be ***kept to a minimum***. In Sweden, the data protection criteria (discussed below, at 6) are set out in the middle of the data protection principles, which can also lead to some confusion.

[56] Already in the current (pre-implementation) law.

In the Netherlands, the law and the Explanatory Memorandum to the law add considerable **clarification or gloss** to the principles, in ways which usually ***strengthen*** or ***tighten*** the principles (as illustrated below, at 5.2). In the UK, the law adds **fixed interpretations** to the principles, which tend to do the opposite, by ***limiting*** the application of the principles. Thus, for instance, the law adds an interpretation of the "first principle" (that personal data must be processed fairly and lawfully), to the effect that such are always to be treated as having been obtained fairly if they were obtained from a person who was "***authorised by or under any enactment [law] to supply it***." With regard to the requirement that data must be processed for "***specified***" purposes, the law adds that this specifying may in particular be done in the information given to the data subject (as discussed below, at 8) *or* in the particulars notified to the data protection authority in the context of "notification" (as discussed below, at 12). This has implications in respect of the use for "not incompatible" purposes, as will be illustrated below, at 5.2.

> CASE EXAMPLE: A major supermarket chain in Denmark used ***credit status data*** to screen job applicants. The data protection authority held that this was allowed only with regard to senior positions. The case was decided under the previous law, and on a different basis - but if the issue arose today, the ruling would be based on the "fairness" principle.

As far the question of **accuracy and up-to-dateness** of data is concerned, there is some divergence with regard to ***non-factual data***, ***reported data*** and ***archived or back-up data***, in that the laws in the common law jurisdictions prescribe certain matters which are left open in others. Thus, both the UK law and the (current, pre-implementation) Irish law - which is not to be changed in this respect - stipulate that data shall only be regarded as inaccurate if they are "***incorrect or misleading as to any matter of fact***" - which means that opinions or assessments of a person can never be "inaccurate" (although they could possibly be challenged if they were manifestly based on incorrect factual information). Other States may be less rigid in this regard. The UK law also adds that ***if data accurately record data obtained from the data subject or a third party***, but are challenged by the data subject, the accuracy principle shall not be regarded as breached as long as (a) the controller took reasonable steps to ensure the accuracy of the data, and (b) recorded the fact that the data subject felt that the data were not accurate - but without actually amending the data. In other jurisdictions the data protection authorities would wish to address the question of what should be the response to such a challenge with a more open mind: they could take the view that in a particular case the controller should take further steps than those mentioned in the UK law - in particular as concerns the recording of data provided by third parties (e.g., the recording by credit reference agencies of credit information provided by companies, or the recording by public authorities of third-party information on persons suspected of making fraudlent welfare claims). The Irish law also says - again, in a provision in the current law which is to be retained in the new (amended) law - that the principle requiring data to be accurate and, where necessary, kept up to date "***does not apply to back-up data***". However, it would be better to clarify that if data are archived or retained for back-up, and date-stamped, they can be regarded as accurate as long as they truly reflect the situation at the time of storage; and that it is only necessary to update such data if they are retrieved.

One could add more examples of specific interpretations or guidance on interpretation of the principles. However, the point to be made is that **by reason of their open-endedness and vagueness, these 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. These points are further illustrated below, at 5.2 and 5.3, while the wider issue of the rather discretionary way in which the laws are applied is addressed at 16.

Greater convergence will require more detailed guidance at European level on the interpretation and application of the principles, although pending that exchanges of information between the Member States, in particular through the Working party, could help generate common views.

5.2 "not incompatible use"

> "personal data must be ... collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. ..." (Art. 6(1)(b), first sentence, of the Directive)

The principle set out above, in English at times referred to as the "**purpose-specification and –limitation principle**" and in German more pointedly as ***Zweckbindung***, is set out in terms identical or very similar to the above in the laws in Austria, Belgium, Denmark, Finland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the UK, and in the proposed new (amended) law in France. In the Greek law, the principle is stated in terms of a "**fairness**" test, in that the law says that personal data, after having been "collected fairly and lawfully for specific, explicit and legitimate purposes" must be processed "***fairly and lawfully ... in view of such purposes***".

However, in spite of the generally similar wording, the very **vagueness** of the principle leaves it ***open to divergent application***. Two matters must be distinguished. First of all, what should be regarded as the "**specified**" purpose. And secondly, how the "[**in]compatability**" of any secondary processing with the primary purpose is to be determined. In practice, the two are closely linked, as can be well shown by contrasting law and practice under the UK and Irish laws.[57]

Specifically, the UK law (uniquely, and as already noted above, at 5.1) stipulates that the purpose of any processing may be specified "in particular" in the information given to the data subject **or** (and this is a crucial point) in the particulars notified to the data protection authority in the context of "notification". In the UK (as elesewhere) the notified purposes are often expressed in broad terms - which means that controllers can claim some considerable leeway with regard to both the primary and any secondary purposes. The implications are well illustrated by the following case under the Irish law which (while otherwise similar to the UK law) does not contain the above stipulation:

> CASE EXAMPLE: The Irish Department of Education used data on its payroll database, which showed which teachers were members of a particular trade union which had engaged in industrial action, to deduct pay from those teachers' salaries for days on which there had been such action. The teachers complained that they had provided the data

[57] The purpose-specification and –limitation principle is already contained in the current Irish law in terms compatible with the Directive, and will be retained in the new (amended) law without modification.

> solely for the purpose of facilitating deduction-at-source of union subscriptions. The Commissioner established that the form through which the data were collected was titled "Authorisation of Deduction of Subscription from Salary", and that the wording of the form "simply mandated the Department to deduct union membership subscriptions from salary". The Department argued that its registration entries specified the purposes of its payroll database in broader terms, and that "since the withholding of the complainants' pay came within the scope of the broad purpose 'administration of teaching staff', ... its use of [the data] was 'not incompatible' with the broad purpose and so no contravention of the Act was involved."
>
> The data protection Commissioner did not accept that argument and held that "the 'specified and lawful purpose' mentioned in [the Irish data protection law] is to be determined by reference to the circumstances in which the data have been obtained. Since the personal data relating to trade union membership had been obtained via a deduction-at-source mandate form, and accepted on that basis, then the 'specified and lawful purpose' for holding those particular data related to the deduction-at-source facility, not any other purpose."
>
> The Commissioner went on to say that the narrow purpose should have been reflected in the registration [notification] particulars: "The Department could not legitimately rely upon this broad description [of purposes in its register entry] to displace the actual purpose for holding the union membership data, or to infer the existence of new "specified and lawful purposes" which were unknown and unthought-of when the data had been obtained." The Commissioner thus held that the department had breached the law.

In the case just mentioned, the Irish data protection Commissioner advised all Government Departments to be more detailed and specific in their notified particulars - but for the present purpose the point is that the determining "specification" is the one provided to the data subjects when the data are obtained, and not the one set out in a controller's notification.[58] In that respect, it should be noted that the list of standard purposes contained in the notification form in the UK (as elsewhere) contains many broadly-phrased purposes.

On the second issue, **"[in]compatability**", the laws and practices in the Member States also vary. Thus, in Belgium the law stipulates that the compatability or incompatability of secondary uses must be assessed in the light of the "***reasonable expectations of the data subjects***". This stipulation derives from a court ruling under the previous law in which it was held, by reference to that test, that a bank could not, without the consent of its customers, use its customers' payment data (which showed how much they paid other companies for certain insurances) to offer them cheaper insurance from its own insurance division.

In Germany, the permissibity or otherwise of secondary processing of personal data for purposes different from the one for which the data were obtained (or disclosed) depends on the application of a variety of (slightly varying) "**balance**" tests, without express reference to "compatability". Basically, data may be used for a different purpose if this serves a (manifest) legitimate [or protection-worthy] interest of the controller or a third party, provided there are no counter-prevailing legitimate interests of the data subjects. These tests were

---

[58] Data on trade-union membership are of course, under the Directive, regarded as **sensitive data**, but that was not at issue in the case at hand (which was of course decided under the current law, which does not contain special restrictions on the matter). Below, at 7.3, it is noted that relevant laws in other Member States (such as the labour code in France) explicitly confirm the position taken by the Irish data protection authority in this case.

developed under the previous law with regard to public-sector processing, and in that context were strictly applied: the interest for which the data could be used had to be manifest, and manifestly stronger than the interests of the data subject against such change of purpose. The extension of these tests to the private sector in principle amounts to a significant tightening of the law in that Member State - but it is too early to see how this test will be applied to the private sector in practice.

The data protection authority in France takes into account, in particular, whether the data subject is under a ***legal obligation*** to provide the data (or has ***little choice in practice***, e.g. as concerns the supply of essential services), and whether the controller bears a special duty of confidentiality (as is the case with data held by ***financial institutions*** or ***medical doctors***, etc.).

The Dutch law elaborates further on ***matters to be taken into account*** in determining whether processing for a secondary purpose is "**(in)compatible**" with the primary purpose for which the data were obtained. It mentions as examples of such matters: the relationship between the primary and secondary purposes; the nature of the data; the consequences of the (secondary) processing for the data subject; as well as the manner in which the data were obtained and the extent to which "suitable safeguards" have been provided to protect the interests of the data subjects. In other words, under the Dutch Law too the question of "compatibility" is addressed very much like the question of "balance" in the context of the data protection criteria. Indeed, in the discussions of various matters in the Explanatory Memorandum the two tests are closely intertwined (not to say confused). According to the Explanatory Memorandum, it follows from the "compatible use" requirement that (e.g.) insurers may not use medical data obtained in the context of an insurance claim in order to take decisions on requests for a ***different insurance*** from the same customer; that data obtained in the context of a sale may not be used (without specific consent) to promote ***unrelated goods and services*** offered by the controller; that the creation of a "***personality profile***" on the basis of such sale data is also "incompatible"; as is the making of ***selections*** in mailings on the basis of "***sensitive***" criteria. Thus, for instance, the authorities have suggested that a pharmacist may not send out a mailing to customers who have boght contact lenses, about a new contac-lens-cleaning fluid (unless the customers expressly and unambiguously consented to this beforehand). In other words, in the Netherlands, the "compatability" test is ***strictly applied***. In Austria and Finland too, certain legal provisions **tighten** the rules on "***purpose-specification***". And in Ireland, the data protection authority also requires that there be a ***close link*** between the primary and secondary purposes; he also (as in Belgium) takes the question of whether data subject can ***reasonably foresee*** a secondary use into account.

> CASE EXAMPLE: The data protection authority in Ireland held that credit card details, provided by a person to a car rental firm when he first hired a car, could not be used in a later situation in which the firm held the person liable for alleged (but disputed) damage to a car used on a different occasion.

If only because of the above-mentioned stipulation about purpose-specification through notification, the UK Information Commissioner is unlikely to go as far as the Dutch authorities in assessing the "compatability" of different products offered by the same company to its customers: if the offering of products by a company to its existing customers is generally allowed (as is the case in the UK, as elsewhere, provided the data subject did not object to such "relationship marketing"), the Information Commissioner is likely to allow the

offering of any product by that company to those customers. The Commissioner, having formally expressed the view that the very concept of "sensitive data" is ill-conceived (see below, at 7 and Part II, at 2.3.4) is also unlikely to adopt the rather rigid position that the use of *any* sensitive data in the making of selections for mailings is *always* "incompatible" with the purpose for which those data were provided.

In Spain, a provision in the data protection law which allowed for widespread exchanges of data between public authorities was partially struck down as **unconstitutional** in the Constitutional Court ruling already referred to above, at 3.4. As a result, such exchanges have become much more limited. Similarly, in Sweden the law (as also explained above, at 3.4) defers to other laws - but this does not mean that the purpose-limitation principle is set aside, but rather, that the legislator must determined the "compatability" of secondary uses of data in the drafting of such other laws.

The Portugese data protection authority also stresses that controllers do not "own" the personal data they control; the authority is therefore also strict about the "compatability" of secondary uses with the primary use for which the data were obtained. Data may thus not be exchanged without further ado, for instance, within a **group of companies**.

5.3 safeguards for scientific processing

> "Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible [with the specified, explicit and legitimate purposes for which the data were collected] provided that Member States provide appropriate safeguards". (Art. 6(1)(b), second sentence, of the Directive)
>
> "Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions [to the in-principle prohibition on the processing of 'sensitive data'] either by national law or by decision of the supervisory authority." (Art. 8(4) of the Directive)

As will be clear from the above, Art. 6(1)(b) of the Directive in principle allows for the further processing of personal data for research purposes, even if the data had not been collected for those purposes, as long as the Member States provide "***appropriate safeguards***". However, the processing of **sensitive data** for such purposes (other than with the consent of the data subjects) is only allowed on the basis of Art. 8(4), also quoted above, i.e. the Member States may only allow this (even with "***suitable safeguards***") with regard to research which serves a "***substantial public interest***."

The Member States have not always (yet) provided "***appropriate***" (or indeed, at times, ***any***) ***safeguards*** with regard to the processing of non-sensitive personal data for research purposes, and to the extent that they have, they have imposed **quite different kinds of safeguards**. They also do not appear to have always appreciated the further-reaching restriction on the use of ***sensitive data*** for secondary research purposes.

Thus, no **safeguards** have yet been provided with regard to secondary processing of personal data for research purposes in Italy and Spain, even though the laws in these countries do allow for such processing without the consent of the data subject. In the Netherlands and Sweden, processing of **non-sensitive data** for research purposes is subject to ***rather limited safeguards*** only, in that the Dutch law merely requires safeguards to ensure that any data used for

research purposes are ***only used for those purposes*** (without otherwise protecting the data subjects); while the Swedish law allows such uses provided the data are not ***used to take decisions*** in respect of the data subjects. The proposed new (amended) law in France also stipulates that personal data used for the (secondary) purpose of statistical, scientific or historical research may not be ***used to take decisions*** in respect of the data subjects - but that law does so **in addition** to the ***special rules*** on such processing, already contained in the current law (as discussed below).

The law in Denmark also stipulates that **non-sensitive data** processed for the secondary purpose of scientific research may only be used "***exclusively***" for that purpose - but if the data are processed for such a purpose by a ***public authority*** and include ***data of a confidential nature*** (which is a wider category than "sensitive data"), the processing must be **notified** to the data protection authority and the latter's **prior opinion** must be obtained (private-sector controllers do not have to notify such operations). With regard to the processing of **sensitive data** (in the full sense) for research purposes, both **public- and private-sector controllers** must obtain **prior authorisation** from the data protection authority. Some further restrictions can be deduced from more general principles in the Danish law. Thus, it can be argued that it follows from the "necessity" principle that data may only be used in identifiable form when this is really needed - and that they should be ***pseudonymised or anonymised whenever possible***. In addition, it follows from the principle that the data may only (exclusively) be used for the research in question that the data may not be used to take decision in respect of the data subjects. However, these implications have not (as yet) been formally spelled out.

The new (amended) law in Ireland, if adopted as currently drafted, will allow the Minister of Justice to prescribe safeguards concerning secondary processing for research purposes - but the law not yet having been adopted, these rules too are not yet in place. In the meantime, the data protection authority does however already stress (like the Danish and other authorities) the need for ***maximum anonymisation or pseudonymisation*** of data to be used for research.

The proviso about research data not being used to take decisions in respect of the data subjects is also set out in the UK law, which adds to this a "**weighted balance**" **test** ("*data are not [to be] processed [for research purposes] in such a way that substantial damage or substantial distress is, or is likely to be caused to any data subject*"). In Germany, secondary processing of personal data for research purposes (without the consent of the data subjects) is also subject to "**balance**" **tests** (although these seem to be less strict) but the law adds some ***further*** (although still not very strong) ***safeguards***, such as a requirement to keep the identifiability of research data to a "minimum" (i.e. to use anonymised or encoded data whenever possible). In Finland, the law lays down certain **general, substantive conditions** (e.g. that "the research cannot be carried out without data identifying the person and the consent of the data subjects cannot be obtained owing to the quantity of the data, their age or another comparable reason") as well a **procedural requirement** that an "***appropriate research plan***" is produced.

By contrast, **detailed rules** have been adopted on the issues in Belgium, which both distinguish between ***fully-identifiable-***, ***pseudonymous-*** (i.e. encoded), and ***fully anonymised data*** and require a review of the research by relevant academic **ethics committees**. In Greece, Luxembourg and Portugal, secondary use of personal data for research purposes requires a ***special authorisation*** from the Data Protection Authority, which if granted may (and will) specify the ***conditions*** under which the processing is allowed. The Austrian law combines a

requirement that ***special authorisation*** be obtained from the Data Protection Authority with detailed ***substantive rules***. In France, there is a law, dating back to 1951 (but amended in 1986), on the creation of **statistics** from public-sector data by the national statistical institute; and a 1979 law on **public archives**, which also deals with the question of ***access*** to such data by academic researchers and historians, subject to ***authorisation*** from the Minister of Culture, with additional safeguards being laid down by the data protection authority as required.

Some countries, like Finland and Germany apply the same rules to the use of **sensitive data** for research purposes without the consent of the data subject, without stipulating that the research must serve an "***important public interest***" or adding ***procedural safeguards***, such as a requirement that research involving such data must be approved by an **ethics committee** as is the case in Sweden (and as is generally required in Belgium, as just noted). In Sweden, a prior check by the data protection authority must always be carried out when personal genetic data derived from genetic investigation are to be processed; when processing other sensitive personal data for **research purposes**, such a prior check must be carried out if consent of the person registered is missing and approval by a research ethics committee has not been given. In France, a separate chapter (already alluded to) was added to the current law in 1994, which deals specifically with the use of **health data** for ***medical research***. The chapter both establishes a special **advisory committee** of experts, and (in addition) requires ***prior authorisation*** for specific research from the data protection authority. Patients can furthermore always ***object*** to the use of their data, even though such use is subject to these safeguards. The rules thus undoubtedly ensure that, in practice, such research is limited to situations in which it serves an "important public interest" and is subject to "appropriate safeguards". Affirming this strict regime, the proposed new (amended) law in that country ***qualifies*** the exception in the Directive, by saying that it applies only if (a) the special rules in this chapter of the law are adhered to and (b) (as already mentioned) provided the data are not used to take decisions with regard to the data subject.

A special Order issued under the law in the UK (further discussed below, at 7.3) itself expressly stipulates that such research is only allowed if it serves a "**substantial public interest**", and the Austrian law too adds that the above-mentioned authorisation can only be granted for research involving such data if the research serves "**important public interests**". The Luxembourg law is somewhat more lax, by allowing processing of sensitive data when this is "***necessary for reasons of public interest such as, in particular, historical, statistical or scientific purposes***" - but the requirement of of a "**prior authorisation**" will in practice nevertheless ensure that such processing can only take place if the public interest in question is evident, and will be subject to appropriate conditions and safeguards (although there is, of course, as yet no practice in this respect).

In Denmark, there are different rules concerning the use of sensitive data for (secondary) research purposes by a controller himself, and concerning the disclosure of such data for such purposes; and the law makes a further distinction between public-sector- and private-sector controllers. Thus, if the data are to be used by a private-sector controller for his own research, this is allowed provided: the data are used ***only*** for the scientific research purpose concerned; that research is of "significant social importancer"; the data are ***necessary*** for that research; and they are not used for other purposes afterwards. It is up to the private-sector controller to make these assessments. By contrast, a public-sector controller needs to first obtain the **opinion of the data protection authority** for such processing. Furthermore, both private- and public-sector controllers require **prior authorisation** from the data protection authority

before ***disclosing*** data for such purposes. The Danish law also adds detailed rules on the establishment and use of **legal information systems** (which, by their nature, contain sensitive data on court cases). The proposed new (amended) Irish law allows for the issuing of **regulations** authorising processing "***for reasons of substantial public interest***" - which of course can include research for such reasons - but the amended law not yet having been adopted, such regulations have also not yet been issued. In the meantime, the data protection authority in that country emphasises the need for **consent** for the use of sensitive data in research. The Irish medical council has also issued detailed guidelines on the use of medical data for such purposes.

Overall, the rules concerning secondary processing of personal data for research purposes without the consent of the data subjects thus **vary very considerably**: some consist of rather general substantive rules, others of more details substantive requirements; some rely on procedural safeguards; and some combine substantive and procedural rules. Some are contained in the data protection law; and some in other laws or regulations.

6. criteria for making processing legitimate [Art. 7]

introduction

It is a unique feature of the Directive (among the international data protection instruments) that it adds to the data protection principles a further list of "criteria for making data processing legitimate". At the request of the Commission, the study examined in particular the rules laid down by the Member States concerning "**consent**", processing in the **public interests** or in the exercise of **official authority**, and processing on the basis of the so-called "**balance**" criterion.

summary of findings

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. Some prohibit processing of certain data in certain contexts (e.g, of ***genetic data*** by ***employers***), even with the consent of the data subjects. Occasionally, this may be controversial, as when one Data Protection Authority effectively banned a television show deemed to be too intrusive of the participants' privacy, even though they had all volunteered for the show.

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 whome the data are disclosed*" 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*** and that the processing must be ***necessary*** for the task or function specified. The laws in some of the first-mentioned States may also have to be read in this way.

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 "**balance**" criterion 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, somewhat differently phrased tests are applied to the **private sector** and the **public sector**, respectively, with the latter in particular appearing to be rather loosely phrased. 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, 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.

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

matters to be further clarified or addressed

The application of the data protection criteria - like the application of the data protection principles, discussed above, at 5 - requires **further clarification**, in particular as concerns the need to impose ***additional requirements***, such as the need to obtain consent in writing in principle or in certain contexts, or conversely when consent can be given in other ways (e.g. by means of a "click" on a computer-mouse), or as concerns the application of the "balance" criterion. Again, if obstacles to the Internal Market are to be avoided, it must *either* be ensured that compliance with a single "applicable" law will suffice in transnational activities - even if this means that processing must be allowed on the basis of (say) "consent", or a "balance" test, which is in accordance with the law in the country where the controller is established, but which would not be regarded as valid in the country where the data are obtained. *Or* the uniform application of the principle in question would have to be ensured through clarification at the European level.

It should also be **made clear, explicitly**, ***in the Directive and in the national laws***, that processing on the basis of the "public interest\official authority" criterion must not only be ***authorised by law*** but also, ***in addition, "necessary"***

for the interest or task concerned; and that if the data protection law in this respect cross-refers to another domestic law, that additional requirement should be read into that other law too.

- o – O – o -

6. criteria for making processing legitimate – detailed findings

6.1 general

> Member States shall provide that personal data may be processed only if:
>
> (a) the data subject has unambiguously given his consent; or
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> (d) processing is necessary in order to protect the vital interests of the data subject; or
>
> (e) processing is necessary for the performance of a task carried out 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; or
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).
>
> (Article 7 of the Directive)

The data protection criteria are contained in the laws of all the Member States, but again with some **significant variations**, both in structure and content.

Thus, first of all, the criteria are set out basically as in the Directive - i.e. as a list of alternative grounds for lawful processing - in the laws in Belgium, Denmark, Finland, Luxembourg, the Netherlands, Sweden and the UK, and will also be included in the new (amended) law in Ireland if that law is adopted as proposed - but in Finland they are set out in the middle of the data protection principles (discussed above, at 5), while in the UK law they are formally linked to the "fair and lawful processing" requirement. The laws in other countries take a more hierarchical view of the criteria: in Austria, Germany and Spain "***consent***" and processing based on a ***law*** or to fulfil a ***legal obligation*** are given primary status (with Spain reversing the order of these two): the other criterion are seen as **exceptions** to these primary criteria. In Greece and Portugal, processing on the basis of ***consent*** is the sole primary criterion: all other processing (including processing on the basis of a law) is seen as an exception to this primary rule. The same will apply in France under the proposed new (amended) law; and applies in Italy with regard to processing in the ***private sector***.

Apart from listing the criteria relating to consent, processing based on law, and processing to protect the vital interests of the data subject, the Austrian law stipulates a general criterion: processing which is required to serve an overriding aim of the controller or a third party - and then brings several of the criteria listed in the Directive, and several more specific criteria - which must be seen as elaborations of the "balance" criterion - under this general heading:

processing necessary to fulfil a public-sector task; processing which is necessary to protect the vital interests of third party; processing relating to a contract between the controller and the data subject; and processing in the exercise or defence of legal claims; as well as processing of data which relate to a "public function" of the data subject. After stipulating the general (primary) criteria of consent and processing based on a law, the German law distinguishes between processing by public- and private-sector controllers, and between processing "for one's own purpose" and for the purpose of disclosing data - and lays down somewhat differing criteria for each which, however, all broadly amount to the application of slightly differing "balance" tests.

Some laws also further elaborate on, or add further provisos to, some of the criteria. This is further discussed with regard to **consent**, processing in the **public interest**, and processing on the basis of the "**balance**" criterion in the next sections.

6.2 consent

> "Member States shall provide that personal data may be processed [*inter alia*] if ...
>
> the data subject has unambiguously given his consent"
>
> (Art. 7(a) of the Directive)

The laws in the 13 Member States which have implemented the Directive, and the proposed new (amended) laws in France and Ireland, 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**.

Thus, as note above, at 6.1, in particular in countries in which data protection is based on a constitutional principle, consent is seen as either **the main criterion**, in the sense that all processing based on any other criterion is construed as an ***exception*** to the primary criterion of consent (France, Greece, Portugal, Italy); or as **one of two main criteria**, with the other one being ***authorisation by law*** (Austria, Germany). It follows from this that the other criteria must be ***restrictively interpreted***.

Several laws emphasise the need for any consent to be ***manifestly*** free, specific and informed etc., by including the term "**unambiguous**" in the very definition of consent (Portugal, Spain, Sweden); as noted above, at 2.8, the Luxembourg law includes both the term "**unambiguous**" and the term "**explicit**" in the definition. The laws in Germany and Italy stipulate that consent should (in principle) be **in writing** (while allowing for the giving of consent on the Internet by means of a "mouse-click").

By contrast, as also noted above, at 2.8, the UK law, the proposed new (amended) Irish law, and the proposed new (amended) law in France all fail to define the concept of "consent" - but they differ in respect of processing on the basis of consent. In the UK law, the provision allowing for processing of (non-sensitive) personal data merely mentions "**consent**" as one condition for processing - which contrasts with the condition for processing of ***sensitive data*** which refers to "***explicit* consent**" (as further discussed below, at 7.2). Guidance on the law, issued by the UK data protection authority, consequently suggests that consent for the

processing of non-sensitive data may, in certain circumstances, be ***implied***.[59] The proposed new Irish law, however, uses the words "***explicit* consent**" both in this regard and in connection with processing of sensitive data. In Ireland, "consent" can therefore clearly not be ***implied***, other than for the most ***obvious, primary purpose*** of the processing. As the data protection authority put it (in the rather particular context of codes of conduct, as further discussed below, at 15):

> "The general, common-sense rule is that an individual's clear consent may be taken as implicit, in the case of the primary purposes - such as the provision of medical care by a GP [a medical doctor], or the provision of telephone services (including necessary billing arrangements) in the case of a telecommunications company. Clear consent may also be inferred from a long-established course of dealings with existing customers, such as bank customers, who have not objected to certain uses of their data over that period. However, secondary uses of personal data will invariably need to be drawn clearly to people's attention, together with an opportunity to signal consent, before clear consent for such purposes can be said to have been established. The EU Directive [*sic*], with its reference to 'unambiguous consent' as a general rule, makes clear that positive 'opt-in' consent - as opposed to passive 'opt-out' consent - will need to be relied upon to a greater extent than before.

The data protection authority concludes that matters such as disclosures of personal data for the (secondary) purpose of direct marketing thus require an "**opt-in**" rather than an "***opt-out***" (as further noted below, at 9.3). However, in view of case-law under the current (pre-implementation) law - which does not yet include the data protection criteria - the term "explicit" will not necessarily be read as requiring consent **in writing**:

> CASE EXAMPLE: The police in Ireland (called *An Garda Siochana* or simply *Garda*) routinely passed on data on victims of crime to a charity, Victim Support. The data protection authority intervened and stressed that consent was required for this. When demand for the service declined by 70%, he discussed the matter with the police and the charity. It transpired that following his earlier advice, the police would only pass on data on the basis of ***written consent***. The data protection authority "explained that consent, at the scene of a crime, need not necessarily involve the completion of a formal consent form by the victim. In the first place, there would be no difficulty with An Garda Siochana routinely informing victims about the useful support services available from Victim Support. Moreover, victims could be informed that it was Garda policy to refer them to this organisation, if the victims were happy to indicate - ***whether verbally or in writing*** - their consent to this. Reasonable steps would, of course, have to be taken to ensure that victims did not feel coerced or pressurised into availing of this service, if they did not want to." The police was also advised "that the relevant Garda file, or the relevant entry on the Garda 'Pulse' computer system, should clearly indicate the type of consent received from the victim."

In France, as already mentioned above, at 2.8, it follows from the general legal approach to the question of consent (e.g. in civil law) that - in spite of the absence of a specific definition

[59] If this were taken to mean that consent could be inferred from silence and inaction on the part of the data subject (e.g. from the mere fact that a data subject did not respond after being informed by a controller that he wanted to use the data subject's data for a certain, previously undisclosed purpose), this would be doubtful in terms of the Directive, which (in the definition of "consent") requires that the data subject's "agreement" to any processing be "signified". Presumably, the UK data protection authority's guidance must be read as meaning that a data subject's consent can be inferred from signals from the data subject which imply his agreement, even though such signals may not be very "explicit".

- **consent** for the processing of ***non-sensitive data*** will only be regarded as valid if it amounts to a "***freely given, specific and informed*** indication of" the "wishes" (*volunté*) of the data subject - but that this *volunté* can be expressed in a variety of ways and that (other than with regard to "sensitive data", for which it needs to be "express", as discussed below, at 6.2) it therefore does not necessarily need to be put in writing. Thus, for instance, if a person was ***informed*** of an intention on the part of a controller to use his (non-sensitive) data for direct marketing purposes, and was ***offered an opportunity to object*** to this use (e.g., by means of a "negative tick-box" on a form), yet ***did not use this opportunity*** (i.e. by returning the form without the box being ticked), his **consent** to the dm-use of his data can be ***inferred*** from this (in)action.

In Germany, a request for consent for a separate purpose than the primary purpose must be **specially emphasised** in printed forms etc. – but in that country (and elsewhere), there is some lack of clarity as to whether the granting of one's consent to such secondary processing, unnecessary for the primary purpose of an agreement, may be made a ***condition*** for the entering into of the primary agreement: this is regarded more as a matter to be resolved in terms of "unfair" (invalid) terms and conditions than as a data protection issue.[60] Under the previous law in the UK this was lawful, unless there was some abuse, e.g. if the controller had a monopoly. The Irish data protection authority s however is strict in this regard - both as concerns the need to especially emphasise that data are requested for a secondary purpose, unrelated to the primary purpose for which the data are collected, and as concerns the permissibility of making the provision of such data for such secondary purposes a condition. In principle, he will not accept the latter unless the primary and secondary purposes are closely related.

In Denmark, consideration had to be give to the question of when a person should be regarded as old enough to give (valid) consent.

> CASE EXAMPLE: A Danish Child Helpline has set up a website where they can be contacted by children with problems. The question arose whether the children who provided information through this website had given valid consent for the processing of their data by the organisation. The data protection authority ruled that if they were capable of logging on to the website independently, they should in general be regarded as capable also of giving their consent to the processing.

This contrasts with the situation under the proposed new (amended) law in Ireland, under which processing of data on a data subject **under 18 years of age** requires the consent, not of that data subject, but of "***a parent or guardian or a grandparent, uncle, aunt, brother or sister of the data subject***" (presumably, provided that the other person *is* over 18). This can lead to problems, as in cases of the kind just mentioned in Denmark, but also in connection with simple commercial transactions or interactions with public authorities - but there is of course no practice in this respect as yet.[61][62]

---

[60] The German Telecommunications Data Protection Law *does* prohibit the requiring of consent for secondary processing as a condition for the provision of a service.

[61] The Irish law also stipulates that consent is to be given by a parent or guardian (or other relative) "if the data subject is **mentally or physically incapacitated** to such an extent as to be likely to be unable to appreciate the nature and effect of such consent" - but this is uncontentious and also applies (even without being expressly stated) in the other Member States.

[62] It is of interest to note that the French data protection authority also dealt with a **child abuse helpline**, but that in that case the question of **consent** does not appear to have been an issue. Rather, the authority's

Several countries make clear that even if a controller obtains the consent of the data subject, there are still ***additional requirements***, and that processing which does not meet those additional requirements is unlawful irrespective of the consent. Thus, the law in Spain stipulates quite generally that processing by private-sector controllers must be "***necessary*** for the success of the **legitimate activity and purpose** of [the controller]". Processing which does not meet this condition is not allowed even with the consent of the data subject. In other countries, this principle is applied more specifically in certain contexts. The law in Finland thus quite strictly limits the processing of personal data on **employees** by employers; the latter may not ask for ***genetic information*** in particular, not even with the (free, express, etc.) consent of the employers. Similarly strict rules apply with regard to the processing of various kinds of sensitive data by employers in France, as further noted below, at 7.3

The idea that the State is, at times, in a better position than the individuals concerned to judge whether processing of their data should be allowed can have far-reaching consequences. Thus, in Greece, the Data Protection Authority effectively prohibited the screening of the television show "**Big Brother**" - in which a group of volunteers stays in a house while being under constant camera surveillance, with the pictures and sound being transmitted over the Internet and on television, in the hope of winning a major cash prize - because the screening (i.e. the recording and transmission of the sound- and image data in question) amounted to an unwarranted interference with the contestents' constitutional right to privacy, which was so grave that they could not waive this breach of their rights. This raises the question both of whether (and if so when) the State can thus override the free consent of data subjects, and the further question of whether the Data Protection Authority is always the appropriate body to decide such matters.

In that respect, it is of interest that the proviso in the Directive to the provision allowing for the processing of "**sensitive data**" with the "***explicit consent***" of the data subject - "*except where the laws of the Member State provide that the [in-principle prohibition on the processing of such data] may not be lifted by the data subject's giving his consent*" - which was included in the Directive at the behest of Denmark because the previous law in that country contained such an exception, is not in practice widely relied upon by Denmark under its new law. One example of the application of this rule in Denmark could be the stipulation in a separate law that employers are not allowed to process medical data on their employees unless there is a clearly demonstrated specific need to do so with regard to the specific employee and his specific activities: this rule cannot be overridden by the data subject's consent. Under the data protection law itself, the authority prefers to rely on the data protection principles (in particular the principle of "fairness" or "good practice") to prevent or stop processing - as it did in the case of the use of credit reference data in the selection of candidates for employment by a major supermarket chain, mentioned earlier.

It may in that respect be noted that the laws in several Member States - Greece, the Netherlands, Spain - stress that "consent" which does not meet the requirements of the law (and the Directive) must be regarded as ***null and void*** (i.e. not just as ***voidable***). The laws in Austria, Denmark, the Netherlands, Spain and Sweden add that consent to processing "***may be***

---

inquiry focussed on the **disclosure** of data by the telephone counsellors to various professionals and institutions (CNIL, 21st Annual Report, 2000, p. 60ff).

revoked at any time" (albeit without retrospective effect, as most make clear). The UK data protection authority has said, somewhat more ambiguously:

> "Even when consent has been given it will not necessarily endure forever. While in most cases consent will endure for as long as the processing to which it relates continues, ***data controllers should recognise that the individual may be able to withdraw their consent***."

She has however not further clarified when they may (or may not) be able to do so.

6.3 processing in the public interest or in the exercise of official authority

> "Member States shall provide that personal data may be processed [*inter alia*] if ...
>
> processing is necessary for the performance of a task carried out 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) of the Directive)

The laws in Belgium, Denmark, Greece, Luxembourg, the Netherlands, Portugal, and Sweden repeat the above-mentioned criterion *verbatim*, without additional clarification. The main point to be made in respect of these laws is that the use of the term "***necessary***" in these laws implies that the justification for processing on this basis is (in principle) subject to **judicial review**. The UK law refers in somewhat more elaborate terms to processing which is "***necessary***" for the ***administration of justice***; for the exercise of "***any functions conferred on any person by or under any enactment [law]***"; for the exercise of "***any functions of the Crown, a Minister of the Crown or a government department***"; or for the exercise of "***any other functions of a public nature exercised in the public interest by any person***". The proposed new (amended) Irish law lists the same matters in similar terms (but of course without references to the Crown; instead the Bill refers to the Government). The proposed new (amended) law in France sets out the criterion in very similar (albeit not quite identical) terms to the ones used in the Directive (it refers to a "***task in the public interest***" only), but crucially also requires that the processing be "***necessary***" for the task concerned. Under the current (pre-implementation) law, the data protection authority already closely scrutinises the need for specific processing operations (and for the data used in such operations) in support of public sector tasks, because of the general requirement that all such processing (unless specifically authorised by statute) be based on a ***regulation***, adopted after the data protection authority has first given its ***prior opinion***. In practice, draft regulations are invariably amended to conform to the opinion of the authority.

The laws in Austria, Finland, Italy, Spain and Germany all also contain the "public-interest task"-criterion, but with some further modifications, additions or qualifications.

Thus, the law in Austria allows processing by **public authorities** in the kinds of contexts envisaged by Art. 7(e) of the Directive only to the extent that the data are "***essential***" for the exercise of the tasks or functions concerned, and only insofar as **these tasks or functions** are specifically laid down ***by law***. **Private entities** may also only process data in such contexts if this is "***specifically authorised by law***". The law in Finland similarly only allows for processing for the kinds of tasks concerned to the extent that this is based on the provisions of a ***law*** and ***necessary*** for whatever is specified in that law, *or* if the processing is ***necessary*** for

compliance with a ***task or obligation*** which the controller is bound to carry out by virtue of a ***law*** or because of an ***order*** issued on the basis of a **law**. Otherwise, a ***permit*** is required from the Data Protection Authority. The law in Italy contains similar constraints, over and above the rather loose wording in the Directive.

As already noted above, at 5.2, the Spanish law as originally adopted used to allow the **widespread disclosure** of data between public authorities on the basis of ***subsidiary regulations*** - but the Constitutional Court, in the ruling referred to in that section and discussed in more detailed at 3.4, held that the wording of the relevant provision was too vague and ***unconstitutional***. As a result of this ruling, the criterion discussed here (processing in the public interest or in the exercise of official authority) must now be **strictly circumscribed** in a law, and if such processing is allowed on the basis of delegated powers, the latter can only deal with secondary and auxiliary matters. As a result, the law now clearly complies with the "necessity" test in the Directive and with the corresponding Spanish constitutional-, as well the general European principles mentioned at 3.4.

As noted above, at 3.4, in Sweden processing may be authorised by any other law or regulation adopted by the Government: the data protection law as such does not stipulate that other laws or regulations authorising processing in support of an official task or function must limit such processing to what is "necessary" for the task or function concerned. However, as also explained at 3.4, the general constitutional-legal approach adopted in that country too nevertheless ensures that this will be the case.

The law in Germany also allows processing for the kinds of purposes envisaged in Art. 7(e) of the Directive whenever this is **authorised by *special rules in other laws*** - but as noted above, at 3.4, such processing is subject to the constitutional requirements concerning "***necessity***" and "***proportionality***" - which should ensure its conformity with the Directive too.

6.4 balancing of interests

> "Member States shall provide that personal data may be processed [*inter alia*] if ...
>
> processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."
>
> (Art. 7(f) of the Directive)

The "balance" criterion, set out above, is contained in identical or similar general wording in the laws of eight Member States: Belgium, Denmark, France (in the proposed new law), Luxembourg, the Netherlands, Portugal, Sweden and the UK. The laws in Belgium and the UK make provision for the issuing of further rules on the application of this criterion, but this has not yet been done. The proposed new (amended) law in Ireland similarly envisages the issuing of further regulations specifying "particular circumstances in which [the 'balance' criterion] is, or is not, to be taken as satisfied" - but the law not yet having been adopted, these regulations too have of course not yet been issued (although consultation on the application of this criterion, and on the need for such regulations, is taking place). In Denmark the law also allows for the issuing of further rules based on the "balance" criterion,

but this power is limited to the issuing of further rules relating to marketing. The principle can be related to the principle of "fairness" or to the other data protection principles:

> CASE EXAMPLE: In Denmark, the "balance" criterion has been relied upon, in conjunction with the "good practice" principle, to issue guidance on **surveillance in the workplace** (as further discussed below, at 10.4). Specifically, it has been held that employees must be ***informed*** of such surveillance, and that monitoring of emails must be limited to ***professional*** [i.e. not private] ***emails***. If these conditions are not met, the processing is "unfair" (contrary to good practice) and cannot take place on the basis of the "balance" criterion; if they are met, it can take place on that basis (in principle).

Further clarification *has* been provided in the Explanatory Memorandum to the Dutch law which mentions as matters to be taken into account: 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***. Also relevant is whether the processing is in accordance with a relevant ***code of conduct*** (in particular, of course, if the code has been positively assessed by the Data Protection Authority). In the other countries just mentioned, similar matters are likely to be taken into account.

In Germany, a "balance" test applies in the above-mentioned general terms only to the **private sector**. In applying this test (which was already contained in the law before this was brought into line with the Directive), the courts have again taken the same kinds of matters into account as are listed above. With regard to the **public sector**, the German law contains a series of ***other (somewhat differently worded) "balance" tests*** - which apply to various kinds of processing which in terms of the Directive should be subject to a "***necessity***" test.

In the other Member States, the "balance" test is applied **more restrictively**, and\or subject to **further formal requirements**. Thus, in Greece, the law ***tilts the "balance"*** strongly towards the data subject by allowing processing only if "the processing is ***absolutely*** **necessary** for the purposes of a legitimate interest pursued by the controller or a third party or third parties to whom the data are communicated and on condition that such a legitimate interest ***evidently*** **prevails** over the rights and interests of [the data subjects] and that their fundamental freedoms are ***not affected***." In Spain, the "balance" test applies first of all to data obtained from a limited range of "**publicly accessible sources**", such as directories or newspapers. In addition, there are some special provisions on **credit and creditworthiness**, and on data used for **insurance** purposes, which also lay down guarantees aimed at striking the balance between the legitimate interests of controllers and data data subjects.

In Italy, the "balance" test only applies in **cases specified by the Data Protection Authority**, while under the Finnish law, controllers need to obtain a **permit** from the Authority if they wish to rely on that test (but the law also contains four special provisions allowing for processing in certain circumstances, such as a customer relationship, which can be said to be specific examples of the application of that test).

7. processing of sensitive data [Art. 8]

introduction

The Directive lays down additional conditions (over and above the usual "criteria for making processing lawful", discussed above, at 6) for the processing of so-called "**special categories of data**" (usually referred to as "***sensitive data***"). The study looked at the **kinds of data regarded as "sensitive" or "special"** by the Member States; at the extent to which the Member States have adopted the approach in the Directive of imposing an **in-principle prohition** on the processing of the main categories of sensitive data, subject to ***specific exceptions***; and then looked in more detail at the **special rules** in the laws of the Member States concerning the processing of sensitive data to comply with obligations under ***employment law***; the special exemptions provided for with regard to ***processing "for reasons of substantial public interest"***; concerning the ***processing of data on criminal convictions (et al.)***; and on the use of ***national identity numbers***.

summary of findings

The Member States **agree** on the main categories of data to be regarded as "***special***" (or "***sensitive***") ***data***, in that they all regard the categories listed in the Directive as such - but some add ***further categories***, or treat certain categories specially even if they are not formally included in the concept of "sensitive data". This concerns data on ***debts***, ***financial standing*** and the payment of ***welfare*** (social security) ***benefits*** in particular. Some States also treat data on criminal convictions etc. as part of the general category of sensitive data - which means that such data can be processed on the basis of the same exceptions (special criteria) as the other sensitive data.

The laws in the Member States **all follow the basic approach of the Directive**, in that they all ***in principle prohibit*** the processing of sensitive data, subject to certain especially listed ***exceptions***; and they all also set out these **exceptions** in ways corresponding to the ones listed in the Directive (with some **variations** or **additions**).

Although the laws in several of the Member States contain provisions concerning the processing of sensitive data to meet the requirements of **employment law**, on the lines of the Directive, these laws provide little specific detail in this regard. Some envisage the adoption of special rules (or a special law), but this has not yet been done. In the meantime, the matter is **mainly left**

to the special laws which apply in this field - such as ***equal opportunities-****(anti-discrimination-)* ***legislation*** and special legislation in continental-European countries on the issuing of "**certificates of good behaviour**". Overall, the situation in this regard is therefore still very much determined by separate - and thus **divergent** - **provisions in *other laws*** than in the data protection laws implementing the Directive, without the data protection laws, or more specific rules issued under the data protection laws (as yet) providing much guidance in this respect.

Several of the data protection laws of the Member States envisage the issuing of decrees or other subsidiary rules concerning the **processing of sensitive data for important public interests** - but this has only been done in two Member State, and in the rules in question, the standards are somewhat ambiguous. Several laws similarly allow for the issuing by the national Data Protection Authority of specific *ad hoc* **authorisations** - but the Commission has not been notified of any. One Member State provides for the issuing of ***permits*** to **human rights organisations**, but this is in itself controversial and may contravene the European Convention on Human Rights; none have been applied for. However, as noted in other sections, ***several of the data protection laws in the Member States quite generally defer to any other domestic laws or –rules - and many of these do authorise the processing of sensitive data***. Such other laws or provisions ***should*** have been notified to the Commission, but they have not always been notified (partly because in several countries the other laws in question are being reviewed). Until these matters have been properly notified, this area will **remain obscure**, but it is clear that until such laws have been properly reviewed, ***substantial differences*** will remain in the rules they stipulate.

The laws in the Member States examined so far ***differ substantially*** with regard to their approach to the processing of data on **criminal convictions etc**. Some include such data in the general category of "***sensitive data***" (which can have repercussions, in particular as concerns the permissibility of such processing with the consent of the data subject), while others extend more special rules on criminal convictions to data on ***other legal disputes*** or to data on "***serious social problems***" or "***purely private matters***". The laws also apply **quite different standards** to the processing of such data. Some permit ***any processing*** of such data if it is *"**authorised by or under any legal provision***", or for any "***purpose specified by law***"; or allow it on the basis of ***vague and subjective "balance" tests***; while others lay down strict "***necessity***" tests and\or require that controllers (especially in the private sector) obtain ***special permits*** or ***authorisations***. There are therefore still clearly **substantial differences** between the laws of the Member States in this respect.

There are ***different basic approaches*** to the use of **national identity numbers**, with some Member States allowing for the widespread exchange of such a number between public administrations if this facilitates their work, and others taking a restrictive approach, under which the use of such numbers is (to be) regulated more precisely. Some countries allow the use of such a number in the private sector with the consent of the data subjects, while others are again more restrictive, fearing in particular that the use of such a number can too easily lead to interconnections of databases and unchecked disclosures of data.

matters to be further clarified or addressed

It is clear that in many respects the laws of the Member States do not yet provide for any - let alone for "**adequate**" or "**suitable**" - **safeguards** with regard to the processing of sensitive data for employment purposes or other reasons of substantial public interest, or with regard to the processing of data on criminal convictions etc. This means that ***they should amend their laws, or adopt rules or decisions under their laws, to provide such safeguards***. Given the vagueness of the terms used by the Directive, it would again be useful if there would be ***central guidance, at European level***, in this respect. However, in this respect that is more **complicated** than usual.

In particular, it should be noted that the exceptions concerned are important ones, in that they touch on particularly sensitive matters, but also that they relate very closely to **other fundamental legal matters in the Member States** (employment law, rules on certificates of good behaviour, rules on the use of the national identity number, etc.). This makes the application of a ***foreign law*** to such matters particularly difficult.

- o – O – o -

7. processing of sensitive data – detailed findings

7.1 categories of data considered to be "special"

> '**Special categories of data'**: "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." (Art. 8(1) of the Directive)

Most of the laws of the Member States regard the same categories of data as "special" or "sensitive" as are listed in Art. 8(1) of the Directive, quoted above. However, there are some differences as to when information relating to such matters must be regarded as "special" or "sensitive"; and some laws add further categories of data to the list.

The laws of Belgium, Denmark and Sweden repeat *verbatim* the wording in the Directive on data "**revealing**" the above personal attributes, and apply this to the same categories of data as are listed above - except that the Belgian law is more specific as concerns ***medical data***. The Italian law also almost follows the Directive word for word, but would appear to be even stricter by referring to data "***capable of revealing***" the various matters; and the Spanish law too is very close to the Directive by applying "special protection" to data which "**reveal**" "**ideology, *trade-union membership, religion or belief***", or which "***refer to***" racial origin, health or sex life. The proposed new (amended) French law uses slightly different terms than are used in the Directive ("*des données qui font apparaitre*" rather than "*qui révèlent*") but they mean the same thing. Indeed, as further noted below, the law expressly clarifies that data are to be regarded as sensitive if they "reveal" the matters listed, "***directly or indirectly***".

It should be noted that the fact that these Member States dutifully repeat the categories of "sensitive" data listed in the Directive does not mean that they are happy to do so. For instance, in Denmark, information on a person's **trade-union membership** was not regarded as "sensitive" until the Directive stipulated this - and the application of the special (strict) rules to this category is not always deemed to be necessary. This has caused some problems about the publishing of membership lists of such bodies (for which consent is required now that the fact of membership if regarded as a "sensitive" bit of information).

Similar seemingly minor textual differences can be found in other laws. The Austrian and German laws both refer to data "**on**" the matters concerned (which is surprising because the German version of the Directive clearly speaks of data "***revealing***" them), while the Dutch law uses the phrase "data ***concerning***" these matters, the UK law and the proposed new (amended) Irish law use "***as to***", and the Greek law "***relate to***". The laws in Finland and Greece too use the words "data ***relating to***" the matters listed, but add further matters, as discussed below. The Luxembourg law refers to **processing** which "***reveals***" the sensitive matters listed.

The various words used - "revealing", "referring to", "relating to", "as to", "on" - would appear to be very similar. However, the terms can have implications, in particular as concerns matters which can be said to ***indirectly "reveal"*** certain sensitive matters. Thus, the fact that someone regularly buys kosher or hala'l meat, or subscribes to certain magazines, or visits certain websites, may not be information "on" or "as to" that person's beliefs or (e.g.) sexual interests or "sex life", but such a fact can be said to nevertheless "**reveal**" such sensitive information. Photographs and video-images also always "reveal" a person's race. These

textual variations therefore do create **divergencies** in the substantive application of the laws. The same can be said concerning the wording of the Luxembourg law: it suggests that data on the sensitive matters listed are not necessarily caught by the provision, unless the ***processing*** of those data "reveals" the sensitive matter. By contrast, as just noted, the proposed new French law expressly stipulates that data which "***indirectly***" reveal sensitive matters are also subject to the in-principle prohibition.

Further **divergencies** arise from the fact that some laws add ***further categories*** to the defined list of "sensitive data". Specifically, the Finnish law treats data on "***social affiliation***", "***treatment***" and "***social welfare benefits***" as **sensitive**; and Greece too regards ***membership in* any *association*** and data on "***social welfare***" as such. This means that the rules on the processing of sensitive data in these countries apply to data to which the comparable (strict) rules in other Member States do not apply. The Portugese law includes in the list of data to be regarded as sensitive, information on "**private matters**" - but without clarifying what this covers. It is clear from the Constitutional Court judgment noted earlier (above, at 3.4) that video surveillance is regarded as, by its very nature, touching on "private matters". The data protection authority would extend this to mobile 'phone positioning data, but does not regard financial data as (purely) "private" (at least not if it is limited to a general indication of income levels). But this clearly leaves a wide "grey" area - e.g. is the fact that someone is a smoker "private"?

In Luxembourg, the Netherlands and in Portugal, **genetic data** are formally defined as data on ***health*** (Luxembourg, Netherlands) or on ***health and sex life*** (Portugal]) and thus brought within the category of sensitive data, while in Sweden the processing of such data is specially regulated, although they are not formally regarded as falling within the specific category to which the rules on "***sensitive data***" apply. The law in Luxembourg also defines "**genetic data**" as "***information of inherited characteristics of an individual or a specific group of individuals***".

Some countries also include in the general list of "**sensitive data**" the special categories of data relating to ***criminal convictions*** etc., addressed in Art. 8(5) of the Directive. As further discussed below, at 7.5, this too creates **divergencies**, in particular as concerns the permissibility of processing such data with the consent of the data subjects.

Finally, it must be noted that several countries impose special restrictions on certain categories of data which are not formally included in the list of "sensitive data" in Art. 8(1) of the Directive. Data on **purely private matters**, **creditworthiness** or **debts** are thus subject to special restrictions in the laws of Denmark, Finland, Greece, the Netherlands and Portugal. In France, such data are regarded as subject to ***special obligations of confidentiality*** (in particular when processed by financial institutions), and thus subject to **strict scrutiny**, in particular as concerns ***disclosures*** and\or ***secondary uses***.

By contrast, the UK data protection authority (the Information Commissioner) has expressed fundamental doubts about the need for treating certain data as (always) special:

> "The concept of special or sensitive categories of data is a traditional feature of data protection law but is **misguided**. It means that even relatively benign information has to be afforded special treatment. ***Personal data are sensitive because of the circumstances in which they are processed not simply because of their content***. For example personal

data revealing religious beliefs are a special category. Can there be any real justification for affording special treatment, beyond the usual data protection requirements, to the Church of England processing a list of its clergy? On the other hand because financial information is not a special category no special protection is afforded to information on a person's income and outgoings. The absence of special provisions for sensitive data under the Data Protection Act 1984 did not lead to any obvious disadvantage for individuals. The interpretation of requirements such as 'fair processing' and 'appropriate security measures' in the light of the nature of the data and the circumstances of processing is the way to approach the problem."

7.2 in-principle prohibition\exceptions generally

"1. **Member States shall prohibit** the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. **Paragraph 1 shall not apply where**:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that' the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims."

(Art. 8(2) of the Directive)

The processing of sensitive data of the kinds mentioned in Art. 8(1) touches on sensitive constitutional issues in the Member States. Some laws reflect this in special provisions. Thus, the Spanish law re-affirms a constitutional stipulation that **no-one may be forced to reveal his religion or beliefs** (and adds that individuals must be ***advised*** of this if they are asked for such information); and stipulates (also because of constitutional imperatives) that **the creation of files solely for the purpose of listing the** "**ideology, trade-union membership, religion, beliefs, racial or ethnic origin or sex life**" **of individuals** "**remains prohibited**." The Danish law contains a similar (if more limited) provision, according to which "***no automatic filing systems*** may be kept on behalf of a ***public administration*** containing data on **political affiliations** which are not open to the public." In Portugal, the Constitution contained a particularly strict provision prohibiting the storing of sensitive data which had to be relaxed in order to allow the adoption of a law in conformity with the Directive.

Otherwise, the laws in the Member States **all follow the basic approach of the Directive**, in that they all ***in principle prohibit*** the processing of sensitive data, subject to certain especially listed ***exceptions*** (in Austria, this is done by stipulating that constitutionally-protected privacy ["secrecy"] interests of the data subjects are not affected if the processing falls within one of the listed categories - but the effect is the same).

They also all set out **exceptions** corresponding to the ones listed in Art. 8(2)(a) – (e), with some **variations** or **additions** - but some are, in certain respects, more particular. Thus, the proposed new (amended) law in France stipulates, quite generally, that the exceptions only apply "***to the extent that the purpose of the processing [strictly] requires it***". While as such this merely re-states the "purpose-limitation" (and thus also applies in the other Member States), it confirms that in France, the exceptions will be strictly applied. Indeed, although the stipulation does not, as such, extend to processing of sensitive data with the (express, written) consent of the data subject, we will see below, at 7.3, that at least in certain contexts, the data protection authority will still assess the need for the processing of sensitive data, even on that basis. It may also be recalled that the French law requires "***express* consent**" for the processing of sensitive data, and that this has been interpreted 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).

The Belgian law refers to associations not just with a "political, philosophical, religious or trade-union aim", but also to associations with a "***cooperativ***e" (*mutualiste*) aim; while the Finnish law does not stipulate that associations of the above-mentioned kind only benefit from the exception if they are "***not for profit***". More importantly, the French data protection authority has stressed that the exception for such associations only applies ***to the extent that the data in question relate directly to the purpose of the association***. Thus, a political party (for example) may not freely collect data on the religious affiliations of its members; and a religious organisation may not record the political views of its adherents.

The Finnish law limits the exception concerning **data made public by the data subject** to ***certain sensitive data only***; the Danish law and the proposed new French law refer to data which are "***made public***" by the data subject, rather than "*manifesty* made public" by the data subject (which is the phrase used in the Directive); while the UK law and the proposed new (amended) Irish law refer (more restrictively) to data which have been "***made public as a result of steps deliberately taken by the data subject***".

The proposed new (amended) law in France refers to processing which is "***necessary***" to protect "**human life**" - which clarifies that the words "***vital interests***", used in the Directive, must be taken literally. By contrast, the proposed new (amended) Irish law extends the exception - contrary to the Directive - to processing of sensitive data which is necessary to prevent ***damage to property***; and applies this not just to cases in which the data subject is physically or legally incapable of giving his consent, but also to cases in which "***the data controller cannot reasonably be expected to obtain such consent***" or where it has been "***unreasonably withheld***".

The Luxembourg law clarifies that processing in connection with (civil-) **legal claims** must not only be "***necessary***" for that aim, but must be "***exclusively***" used for the purpose, and must be ***in accordance with the relevant rules of procedure***.

The Dutch law contains the general exceptions concerning processing of sensitive data with the consent of the data subject, of data made public by the data subjects, and of data used in legal contexts - but is more specific with regard to the other categories, by (in effect) incorporating **detailed rules** issued under the earlier law into the new law. These specify quite precisely ***which kinds of organisations*** can process ***which kinds of sensitive data*** for ***which kinds of purposes***, and subject to ***what kinds of conditions***.

In Denmark, Germany, Greece, Italy and Portugal, the laws lay down **additional formal requirements** for all or certain cases, in that they stipulate that processing of sensitive data (even if it falls within one of the exempted\ permitted categories) may still only take place if the "**prior opinion**" or a "**prior authorisation**" was obtained from the data protection authority (Denmark, public and private sector, respectively); or if a "**prior check**" was first carried out (Germany); or that some in-principle exempted\permitted processing (e.g. by a not-for-profit association) still also requires a **permit** or **authorisation** from the data protection authority (Greece, Italy). In Luxembourg, "**prior authorisation**" is required for processing of sensitive data with the ***consent*** of the data subject, for processing of sensitive information "***manifestly made public by the data subject***", for processing of sensitive data in order to carry out the "***specific obligations and rights of the controller***" (including the obligations and rights under employment law, discussed below, at 7.3), and (as already noted above, at 5.3) for the processing of sensitive (and non-sensitive) data for ***research purposes***. In Portugal, processing of sensitive data on ***important public interest grounds*** and even processing with the ***explicit consent*** of the data subject also, in addition, still requires the **authorisation** of the data protection authority. The French law requires **prior authorisation** for the processing of ***genetic data*** (except for medical purposes) and for the use of ***biometric data*** in order to ***identify*** individuals (which has a bearing on the use of CCTV systems, as will be noted below, at 10.4).

7.3 the processing of sensitive data under employment law

> "[The prohibition on processing of 'sensitive data' shall not apply where] ...
>
> processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards"
>
> (Art. 8(2)(b) of the Directive)

The laws in Austria, Belgium, the Netherlands, Sweden and the UK, and the proposed new (amended) law in Ireland, contain generally-worded provisions on the lines of Art. 8(2)(b), but add little or no detail. The UK law provides for the drawing up of a special Order on this issue, but no such order has been issued (although another Order, on the processing of sensitive data generally, has been adopted, as noted below). The proposed new (amended) law in Ireland also stipulates that the Minister of Justice may either exclude the application of the exception in certain cases, or impose "further conditions" - but the law not having been adopted, no such regulations have of course as yet been issued either. Guidance in Austria is

mainly limited to stipulations about the need to consult the **Workers Council** on any specific rules to be applied within a company. A recent report in Sweden found that there were, as yet, "***no cohesive rules for protection of personal integrity in working life***" and proposed that a special law be adopted on this matter.

As noted above, at 7.2, the law in Luxembourg contains a ***wider* exception**, under which processing of sensitive data is allowed in order to carry out **any** "***specific obligations and rights of the controller***", including "in particular" the obligations and rights under employment law - but as also noted there, such processing is also subject to the procedural requirement of a "**prior authorisation**". The data protection authority can, and will, impose the required safeguards in those authorisations.

The Danish and Finnish laws include specific provisions allowing employers (or controllers generally) to process data on **trade-union membership** - but this is mainly because processing of that particular sub-category of sensitive data is not addressed in the more general employment laws. Some data protection laws - e.g. in Belgium, Greece and Finland - are strict as concerns the kinds of data that employers may process and as discussed above, at 6.1, above, expressly forbid the processing by employers of certain data (e.g. **genetic data**), even with the consent of the data subject. The Luxembourg law - which, as we have seen, contains special, strict rules on the processing of **genetic data**, also does not include processing in the context of employment law in the list of cases in which the processing of such data is permitted. This means that the above-mentioned general exemption relating to "rights and obligations of the controller" does not extend to such data.

In France, the **labour code** contains a range of provisions ***limiting*** processing by employers which can affect the rights and interests of their employees. These stipulate, for instance, that the **Workers' Council** must be consulted on ***technical surveillance of employees*** (as further discussed, with reference to CCTV systems in particular, below, at 10.4); that employers may not collect ***information on employees or job applicants from third parties*** without their knowledge; and - most important in the present context - that any information on employees must be ***[strictly] related to the employment (or prospective employment) in question***. In the latter regard, the data protection authority has held, for instance, that it was improper and unlawful for a recruitment agency to record such matters as ***nationality*** or ***dates of naturalisation***, whether a job applicant had performed ***military service*** or had been a ***conscientious objector*** to such service, or that a person was a ***homosexual***. Indeed, the authority lodged a **criminal denunciation** with the prosecuting authorities in this case. The recording of data on ***ethnic origin***, ***political opinion***, ***religious beliefs*** or a ***physical handicap*** are equally prohibited unless **strictly required** for the job concerned. Information on ***trade-union membership*** may be processed for the purpose of deducting contributions from a worker's salary, but absolutely for no other purpose.[63]

In Germany, too, it is felt that there should be a special employment data protection law covering all the relevant matters in detail, but no such law has yet been drafted. In other countries, such as Portugal, the matter is covered only loosely, by a provision allowing the processing of sensitive data generally on the basis of "a [read: any] legal provision" -

[63] Cf. the Irish case on the improper use of such data, given as an example of a violation of the "purpose-limitation"-principle above, at 5.2.

although the law adds that this is subject to the provision of "guarantees of non-discrimination".

The matter is therefore **mainly left to the special laws which apply in this field** themselves, without the data protection laws adding much clarification on how the stipulation in the Directive is to be applied in the context of those other laws, or indeed without specific reference to such other laws: the processing in question is often covered by provisions allowing the processing of sensitive data where this is ***necessary to meet a controller's obligations under any law***. The special laws concerned are as such not the object of this Study, and some general remarks may therefore suffice.

They include in particular **equal opportunities** (anti-discrimination-) **legislation**. Such laws require employers in companies of a certain size to monitor the ***ethnic composition*** of the workforce. These laws tend to specify that the sensitive data in question must be separated from the other data on employees and may only be used for the statutory purpose concerned. The relevant rules in some countries - e.g. the non-discrimination law in the Netherlands and the Order on the processing of sensitive data in the UK (which elaborates on the rules in the law) - add that such data may not be processed for such purposes if the data subject objects.

Another matter dealt with by special legislation in continental-European countries is the issuing of "**certificates of good behaviour**" by relevant (usually local) authorities, under legislation on **criminal records**. The laws and regulations in question usually **limit** the amount of data on such convictions which is made known to employers and especially prospective employers, and are seen as a means of striking the balance between protecting the interests of employers and the general aim of resocialisation and rehabilitation of offenders.

Overall, the situation in this regard is therefore still very much determined by separate - and thus **divergent** - provisions in other laws than in the data protection laws implementing the Directive, without the data protection laws, or more specific rules issued under the data protection laws (as yet) providing much guidance in this respect. It is furthermore rare for detailed data protection rules to be included in such other laws (although, as we have seen, this has been done in France). In the circumstances, there is **no certainty** that processing "for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law" is limited to what is "***necessary***" to achieve those purposes. At most, a general restriction of that kind may derive from ***constitutional principles*** (as noted above, at 3.4) - but without those laws containing more specific "***adequate safeguards***", as required by the Directive.

7.4 exceptions for reasons of substantial public interest

> "Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down [additional] exemptions [from the prohibition on processing of 'sensitive data'] either by national law or by decision of the supervisory authority."
>
> (Art. 8(4) of the Directive)
>
> "[Such exemptions] shall be notified to the Commission."
>
> (Art. 8(6) of the Directive)

The laws in the Member States implementing the Directive themselves provide for **few specific exceptions** to the in-principle prohibition on the processing of sensitive data, on the lines envisaged in Art. 8(4) - although several of them allow for the adoption of ***subsidiary rules*** of this kind.

The proposed new (amended) Irish law contains special provisions allowing for the processing of sensitive data when this is "***necessary***" for the purpose of assessing or collecting any **tax or duty**, or to determine entitlement to **social welfare payments** (with the "necessity"-stipulation being the only safeguard). The law in Belgium also contains some exceptions with regard to data which are necessary in relation to the provision of ***social welfare*** and ***health services***, but a more detailed decree on the matter, envisaged in the law, has not yet been issued. The law in Belgium furthermore contains a special provision on the processing of data by ***recognised*** **institutions working in the field of sexual crimes**; and also - uniquely - allows for exemptions for the benefit of **human rights organisations**. However, the law makes the latter exception conditional on the obtaining of a ***permit*** by such organisations, which may contravene the European Convention on Human Rights (as further discussed below, at 10.1, with reference also to certain special arrangements made for **Amnesty International** in Denmark). No such permit has yet been sought or obtained. The law in Spain contains one special provision, allowing for the processing of sensitive data by the police "in cases in which it is ***absolutely essential*** for the purpose of a ***specific investigation***". Further special exceptions could be issued in the form of Royal Decrees, but this has again not yet been done. The Austrian law stipulates that if other laws are adopted which authorise the processing of sensitive data, this must be notified to the Commission, but again no such notification has been made. The Luxembourg law allows for the processing of sensitive data in the course of a "**judicial procedure**" or a "**criminal investigation**", but imposes further restrictions on the use of ***genetic data*** in these contexts. The first of these is in accordance with the exception in the Directive relating to "the establishment, exercise or defence of legal claims" (provided that the data are "necessary" for such proceedings, as may be assumed to be the case by virtue of the more general provision on the processing of data in the context of legal proceedings, discussed below, at 7.5), while the second matter is outside the scope of the Directive. And as we have already noted above, at 5.3, a special new chapter was added to the French law in 1994, which allows for the processing of **health data** for the purposes of ***medical research*** (subject to strict substantive and procedural safeguards).

The laws in several Member States - Denmark, Finland, the Netherlands and Sweden – and the proposed new (amended) law in Ireland *do* expressly provide for the issuing of more specific *ad hoc* "**authorisations**" as envisaged in Art. 8(4), but none of these have actually issued them as yet (or if they have, they have not informed the Commission of this).

Exceptions are the UK, where (as noted at 7.1) a **special Order** has been issued on the processing of sensitive data, and France, where special processing of this kind has been authorised by ***special laws*** and (on rare occasions) by ***special decree***.

The UK 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**".[64] These provisions are thus examples of the kinds of special cases to which Art. 8(4) alludes. In each case, the Order (a) defines the processing, and (b) sets out the relevant condition or conditions (i.e., in terms of the Directive, the relevant safeguards). One of these has already been dealt with, i.e. processing of sensitive data for the purpose of **research** which is ***in the subtantial public interest*** (see above, at 5.3). The remaining four contexts, and the corresponding safeguard(s) or condition(s) which apply to processing in these contexts are:

- processing of sensitive data for the purposes of the **prevention or detection of any unlawful act**, on condition that seeking the consent of the data subject to the processing would ***prejudice*** those purposes.

- processing is required **to discharge functions which protect members of the public from certain conduct** which may not constitute an unlawful act, such as incompetence or mismanagement, again on condition that seeking the consent of the data subject to the processing would ***prejudice*** those purposes.

- **disclosures for journalistic, artistic or literary purposes** of personal data relating to unlawful acts, dishonesty, malpractice or other seriously improper conduct, incompetence etc., on condition that the disclosure is made with a view to the ***publication*** of those data and the controller reasonably believes that such publication would be ***in the public interest*** (this refers to so-called "***whistleblowing***").

- processing required to discharge functions involving the provision of **confidential counselling, advice, support or other service**, on condition that the data subject ***cannot*** consent, or that the controller ***cannot reasonably be expected*** to obtain the data subject's consent, or where obtaining the data subject's consent would ***prejudice*** the provision of that counselling, advice, support or other service.

The Order also allows processing of the ***political views of individuals*** by **political parties** "in the course of their legitimate activities", provided this "does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person." The proposed new (amended) Irish law contains a similar provision, under which additional safeguards may be prescribed for such processing - but with the law not yet having been adopted, these subsidiary rules have also not been yet issued. These (from the point of view of continental-European countries, somewhat unusual) exceptions relate to the time-honoured practice in the UK and Ireland - regarded as part of their democratic history - of political parties listing the political leanings of the population, by household, on the basis of responses obtained in the course of door-to-door canvassing in elections.

The UK data protection authority has raised the question of what exactly is meant by the reference to "substantial public interest" in Art. 8(4) of the Directive, and has suggested that a broad view can sometimes be taken, in that it may be "in the substantial public interest" to allow private-sector controllers to process certain kinds of sensitive data for certain purposes,

[64] Processing for the purpose of promoting equality and non-discrimination (noted above, at 7.2, in connection with employment) is of course also in the "substantial public interest", but this is therefore not stated as an additional condition.

without having to obtain the consent of the data subjects. She illustrated this with reference to the processing by employers of information on employees' sickness:

> "It is ... unsatisfactory that there is no clear basis for an employer to process sickness records of employees without their explicit consent. The Directive requires that exemptions can be laid down only for reasons of 'substantial public interest' but there must be a 'substantial public interest' in allowing employers to keep sickness records on employees without imposing on them unrealistic or meaningless requirements to obtain consent which may only serve to bring data protection law into disrepute. The Commissioner is concerned that in the Order [on the processing of sensitive data: see the text, above] the Government appears to have taken the view that, in most cases, there must be a substantial public interest in processing as a prerequisite of satisfying a condition. If this is derived from the reference in the Directive to 'substantial public interest' it appears to be based on a misinterpretation. The Directive (Article 8(4)) requires that the condition is laid down for reasons of substantial public interest not that all processing under the terms of the condition necessarily meets this qualification."

In France, a number of special laws and decrees can be seen as exemptions of the kind envisaged in Art. 8(4) of the Directive. Apart from the special new chapter in the data protection law itself concerning **medical research**, mentioned above, this includes a law on the regulating **the disclosure of certain medical data to health insurance bodies** (subject to the issuing of an opinion by the data protection authority in specific contexts). Apart from such research-related matters, regulated by law, special exemptions can also be granted by decree, again subject to an opinion by the authority. A (rare) example of such a decree is the one authorising the recording of **civil agreements between same-sex partners** with local courts (which in effect give the parties to such agreements certain rights and obligations akin to spouses). Further decrees (outside the scope of the Directive) relate to ***public security***, the fight against ***terrorism***, ***defence*** and ***State security***.

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 them. 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 and Sweden, and to a lesser extent Finland, Spain and the UK - 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 as noted above, at 3.4, in some (in particular, in Sweden) the authorities are reviewing (or have already reviewed) such other laws to ensure that they conform to the Directive; while in others (such as Austria, Germany and Portugal), the **constitutional status** of data protection should ensure that such other laws and rules conform to the Directive.

Even so, until the Member States fully comply with their duty to notify the Commission of **all legal provisions** and **all *ad hoc* Art. 8(4)-type authorisations** under which senstive data may be processed in their legal system, ***this important area will remain obscure*** and departures from the Directive may occur. As with he exemption relating to employment law, noted in the previous section, there is again **no certainty** that processing authorised in such other laws is truly limited to matters of "***substantial public interest***", or that (even if they do serve such interests), the exemptions are limited to what is "***necessary***" to serve those interests. At least

as long as such other rules have not been reviewed domestically, they will also **differ** in ***many respects***.

7.5 processing of data on criminal convictions and offences

> "Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.
>
> Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority."
>
> (Art. 8(5) of the Directive)
>
> "[Such exemptions] shall be notified to the Commission."
>
> (Art. 8(6) of the Directive)[65]

The laws of Finland, Greece and the UK, and the proposed new (amended) law in Ireland, include data on criminal offences *et al*. in the general category of "**sensitive data**". This can have certain repercussions, in particular in that this means that such data can be processed on the basis of any of the exceptions set out in Art. 8(2) of the Directive, including in particular the **consent** of the data subject. However, in Finland and Greece this is generally unlikely, however, because the laws in these countries lay down special restrictions or are strictly applied. In the UK, it has become a criminal offence to require someone (in particular, a job applicant) to use his right of access to data on his criminal record for the benefit of the third party (e.g. a prospective employer) ("***enforced subject access***"). A similar prohibition is included in the new (amended) data protection law in Ireland - but this is an issue on which consultations are still taking place. In the meantime, the data protection authority in that country encourages other special measures to avoid or alleviate such abuse, as noted below.

The law in Belgium extends the restrictions on the processing of criminal data, in Belgium to data on ***any legal disputes***. The law in Luxembourg stipulates quite generally that the processing of **any personal data** "***in the context of criminal investigations or judicial proceedings***" (i.e. including civil- and administrative proceedings) must be in accordance with the **criminal procedure code**, the **civil procedure code**, and the **law on procedure in administrative proceedings**.

The standards to be applied to the processing of **data on criminal convictions etc.** ***vary considerably***. In Belgium, such data can be processed for "***any purpose specified by law, decree or regulation***" - which is rather lax, as are the "***weighted "balance" tests*** stipulated in

---

[65] In the context of answering a question on the implementation of this provision in the recent Commission questionnaire on implementation, the UK Government noted an anomaly in this provision, in that: "*The drafting of Article 8.6 of the Directive causes doubt about the status of the categories of data mentioned in the question. It suggests that Article 8.5, which refers to the categories of data mentioned in the question, provides derogations from Article 8.1. However, Article 8.1 makes no reference to the categories of data concerned. It is unclear, therefore, how these categories of data should be treated.*"

Denmark and Germany. In Luxembourg, the law says that such data "may only take place on the basis of a ***statutory provision***", while in Denmark, the processing of data from the Central Criminal Register is separately regulated, with the rules differing to some extent between the release of data on criminal convictions etc. to private- or public-sector controllers (the latter being given wider access).

As noted above, the law in the UK includes data on "***the commission or alleged commission of any offence***" in the general list of "sensitive data" and thus allows the processing of such data on the same basis as any of the other kinds of sensitive data listed. The law and the special Order on the processing of such data (already referred to in earlier sections) generally allow such processing if it is in the "***substantial public interest***" and "***necessary***" for the particular interest (or task or function) concerned - but leave the question of when this is the case to the controller (at least in first instance). In the Netherlands, much of such processing is covered by **special laws** which lay down ***strict standards*** - but the law also contains a more **general exception clause** containing very ***subjective and vague*** requirements only.

Some countries lay down stricter requirements, if not for all processing of such data than at least for some. Thus, under the proposed new (amended) law in France, data on criminal convictions etc. may only be processed by ***courts***, ***public authorities*** and other ***public-sector entities*** to the extent that the processing "***takes place within the framework of their legal functions***"; and by others associated with the legal system (including ***lawyers***) to the extent "***strictly required***" for the exercise of tasks carried out on the basis of the law. Such processing (other than by defense lawyers) is furthermore subject to a ***prior authorisation*** to be issued by the data protection authority. In Italy, the processing of data on criminal convictions requires ***special authorisation*** from the Data Protection Authority unless it is specifically authorised by **law**. The same applies in Spain with regard to private-sector controllers (public authorities may process such data provided this is stipulated in the [published] Ordinance covering their processing and provided the Authority has been duly notified). As already noted above, at 7.1, many continental-European countries furthermore have rules on **certificates of good behaviour** which try to strike a careful balance between the conflicting interests involved, in particular in the disclosure of data on criminal convictions in an employment or job-application context. In Ireland, the data protection authority welcomed a new practice of the police authorities, under which they would provide individuals with a "***Character Reference for Emigration***" which (in accordance with the Probation of Offenders Act) did not list "spent" convictions, even though the full police records did contain details on such convictions.[66] The law in Finland (apart from laying down special rules on such certificates) also contains more generally limits on the ***providing of data on criminal convictions by public authorities to private-sector*** controllers, and on the use of such data by ***insurers***. The law in Sweden makes processing of data on criminal convictions by **private-sector controllers** subject to the obtaining of a ***permit*** from the Data Protection Authority. In Greece too, such processing requires a ***permit***, and in Austria, the law lays down both a special ***weighted "balance"*** test and requires relevant controllers to submit the processing to a "**prior check**" as envisaged in Art. 20 of the Directive. In Portugal, the law only allows the creation of "**central registers**" relating to criminal matters by ***authorities especially authorised to do so by law***, and otherwise requires **special authorisation** from the data protection authority. The law is also strict with regard to the processing of such data by the police. The law in Luxembourg, too, only allows the establishment of a "**complete**

[66] Note that there is, as yet, no central criminal register in Ireland.

register of criminal convictions" under the control of "***the competent*** [i.e. legally designated] ***public authority***."

The propriety of the above rules is difficult to assess in terms of the Directive, which strictly speaking only requires "***suitable specific safeguards***" with regard to processing of data on criminal convictions etc. ***other than under the control of official authority***. However, it is clear that there are still **major differences** between the rules in the different Member States on the processing of the kinds of data mentioned in Art. 8(5) of the Directive.

7.6 processing involving a national identification number[67]

> "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed."
>
> (Article 8(7) of the Directive)

Not all Member States have national identity numbers; in several the introduction of such numbers is being discussed. The law in the UK expressly allows for the introduction of special conditions on the use of such numbers, but there is no national identification number in the country. It is however clear that there are **different approaches** to the use of such numbers.

In Ireland, a **Public Service Number** was introduced in 1998 by means of social welfare legislation. This number is used in ***all dealings with public authorities*** - but may not be used by private bodies (or indeed asked for by the police). The data protection authority has, after consultations, stopped some data exchanges between public authorities, but remains concerned about the potential for abuse. The Commissioner hopes to issue a **code of practice** on the use of the number before the end of 2002. He stresses that he is not opposed to the Public Service Number as such - indeed, would not be opposed to a full national identify number - because he feels that this issue is not the existence or otherwise of such a number but the constraints placed on its use, and the effectiveness of the enforcement of such constraints. Some countries, including Denmark and the Netherlands similarly allow for **wide uses and exchanges of such a number between public bodies**, if this is useful for the work of the bodies in question.

The law in Finland stipulates that the use of such a number is generally allowed with the ***consent*** of the data subject, but imposes strict **limitations** on its use otherwise. In Sweden the use of the number, even with the ***consent*** of the data subject, must still be "**clearly justified**". This means, in particular, that the number may not be used to "match" different databases, unless there is clear justification for this. In Greece, Luxembourg and Portugal, "***interconnections***" between files or "***combinations***" of data - which is what an identity number is particularly useful for - requires a **permit** from the Data Protection Authority, and similar restrictions apply elsewhere to the creation of such links.

In France, too, the national identity number, NIR (the R refers to the national **r**epertory for the identification of physical persons, RNIPP), is subject to **limitations**, imposed by the data protection authority. The latter has sought, in particular, to limit the use of the number to

[67] For general background and an overview of the situation a decade ago, see the Council of Europe report, The introduction and use of personal identification numbers: the data protection issues (1991).

clearly specified circumstances, for clearly defined purposes, and has attempted, in particular, to ***prevent the use of the number for the creation of (unregulated) interconnections*** between databases operated by different (mainly public-sector) bodies, for different purposes. However, the authority has also, more recently, warned that the convergence of electronic protocols means that data exchanges are becoming easier also in the absence of any single, central identifiers; and said that there is therefore a need for a fundamental re-appraisal of the issues.

8. informing of data subjects [Arts. 10 & 11]

introduction

The informing of data subjects of various details of the processing of their data is a crucial measure to ensure transparency in data processing: if data subjects do not know that data on them are being processed, for what purpose, and by whom, they cannot effectively exercise their data subject rights and data protection becomes illusory.

The Directive therefore provides detailed guidance on the information that must be provided, and in this 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.

summary of findings

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 - both in circumstances in which data are collected directly from data subjects, and in cases in which data on them is otherwise obtained. They also differ as to the kinds of ***additional information*** that may need to be provided to ensure "fairness" (with some of them repeating the examples given in the Directive, others giving somewhat different examples, and some giving no examples). Some add examples of specific situations in which additional information may have to be given which may not be regarded as situations in which this would be required elsewhere.

matters to be further clarified or addressed

The considerable differences between the laws in these respects create **serious problems** for ***transnational operations*** in which data are typically collected (directly or indirectly) from one country, for the purpose of processing in another. If controllers have to comply with different requirements in different countries for pan-European operations (e.g. for a multinational marketing campaign), this seriously increases costs. If they were to comply only with their local law, this could lead to problems in target countries with stricter laws (unless the "applicable law" rules were clearly and readily accepted - which is however not the case, as noted above, at 4). Greater convergence, and clarification of the requirements in a transnational context, are urgently needed.

- o – O – o -

8. informing of data subjects - detailed findings

8.1 informing when data are collected from data subjects

Article 10
Information in cases of collection of data from the data subject

> Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
>
> (a) the identity of the controller and of his representative, if any;
>
> (b) the purposes of the processing for which the data are intended;
>
> (c) any further information such as
>
> - the recipients or categories of recipients of the data,
> - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
> - the existence of the right of access to and the right to rectify the data concerning him -
>
> in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

The Member States have implemented the above provision (and its companion one, Art. 11, discussed in the next sub-section) **quite differently**. Some stay quite close to the Directive, while others divert considerably from it.

The laws in Austria, Belgium, Denmark, Luxembourg, the Netherlands, Portugal, Sweden and (to a lesser extent) the UK thus more or less follow the stipulations in the Directive that the first two items listed in Art. 10 of that instrument - information about the **identity of the controller** and his ***representative*** (if any), and of the **purposes of the processing** - must always be provided, while **additional information** need only be provided if this is necessary to ensure "***fairness***" - but even then with ***some not insignificant differences***.

Specifically, the law in the UK and the proposed new (amended) law in Ireland appear to ***qualify*** the informing-requirement (contrary to the Directive) by stipulating that the information should be provided "***or made readily available***", and by adding that the information must (only) be provided ***"[in]sofar as practicable***". As far as the additional information is concerned, the Belgian law says that it must be provided *unless* the information is *not necessary* to ensure fairness; and the Danish and Swedish laws that this information must be provided when this is necessary to ***safeguard the data subjects' rights*** (or to enable them to ***exercise those rights***). The Luxembourg law refers to "***any other, additional information, such as***" the matters listed - without alluding to "fairness" (although that may be assumed to be implied). The Portugese law stipulates that if data are collected by means of "**documents**" (such as a form or questionnaire), the information which must be provided must be contained in the document in question, and this is also a requirement of the current French

law which is likely to be retained under the proposed new law (even if the latter no longer spells this out expressly).

The Portugese law also contains a further, unique provision concerning the collecting of personal data "***on open networks***" (such as, in particular, the **Internet**), which stipulates that in such cases:

> "the data subject shall be informed, except where he is already aware of it, that personal data relating to him may be circulated on the network without security measures and may be at risk of being seen and used by unauthorised third parties."

The proposed new (amended) law in Ireland repeats the examples of additional information which may have to be provided to ensure fairness, given in the Directive: information as to the ***recipients or categories of recipients*** of the data; as to ***whether replies are obligatory***; as to the ***consequences of any failure to provide the data***; and as to the existence of the ***rights of access and rectification***. The Luxembourg law adds to this: information on ***the length of time for which the data are to be retained***. By contrast, the laws in Austria, the Netherlands and the UK do not provide any examples. However, in the Netherlands, this is further clarified in the Explanatory Memorandum to the law, in accordance with the Directive. In the UK, the data protection authority (the Information Commissioner) has similarly clarified that:

> "As guidance in this respect the Commissioner would advise that data controllers consider the extent to which the use of personal data by them is or is not **reasonably foreseeable by the data subjects**. To the extent to which their use of personal data is not reasonably foreseeable, data controllers should ensure that they provide such further information as may be necessary."

To this she added:

> "[D]ata controllers should consider what processing of personal data they shall be carrying out once the data are obtained and consider whether or not data subjects are **likely to understand** the following:
>
> a) the purposes for which their personal data are going to be processed;
> b) the likely consequences of such processing; and
> c) more particularly, whether particular disclosures can reasonably be envisaged.
>
> It would be expected that the more unforeseen the consequences of processing the more likely it is that the data controller will be expected to provide further information."

The law in Austria on the other hand does provide examples of the kinds of **situations** in which fairness may require the providing of additional information, i.e. if the data subject could object to the processing, or if it could be unclear whether the data subject is under a duty to provide the data or not, or if the data are to be used in processing by means of interconnected databases (unless the interconnection is provided for by law). The Austrian law also stipulates separately that if a controller sends a message to a data subject, he must "***reveal his identity***" to the data subject in this message, and if the controller has notified his operations, he must in this context specify the **registration number** under which he is registered with the Data Protection Authority (if the message is sent in someone else's name, as in ***host mailings***, it must also still contain this number of the controller as well).

The laws in the other Member States are **more demanding** in that they stipulate that some or all of the **additional information** listed in the Directive - information as to the ***recipients*** of the data, as to the ***obligatory or voluntary nature of a reply*** (and as to the ***consequences*** of a failure to reply), and on the data subject's ***rights*** - must always be provided. The proposed new (amended) law in France requires the informing of the data subject, **in all cases** except when the data subject was already informed (which is stricter than the Directive), of: the ***identity of the controller or his representative***; the ***purpose*** (singular) of the processing; the ***obligatory or voluntary nature of a reply*** and the ***consequences*** of failure to respond; the ***recipients*** or ***categories of recipients*** of the data; and of his ***rights***.[68] The new law also contains a special provision allowing the use of "**cookies**" only if the controller has first informed the user (i.e. a visitor to his website) of the ***purposes of the processing*** and of the ***means available to oppose*** the processing, in "***clear and comprehensive terms***". The webhost may, moreover, not make the acceptance of a "cookie" a ***condition*** for access to the service in question.

The German law requires controllers to always inform data subjects of the (categories of) ***recipients of their data***, and requires them to inform the data subjects also of ***whether they have a legal duty to reply*** (or if not, that replying is voluntary). The Italian law requires controllers to always provide ***all of the additional information*** (unless this is already known to the data subject or would hinder supervisory activities of public authorities). The Finnish law requires the same but adds even further-going requirements about **credit data**. The Greek law stipulates that (all) the information must be given **in writing** and that if data is demanded on the basis of a legal obligation, the controller must inform the data subject of the ***specific legal rule*** which requires the providing of the information. The Spanish law too requires that all the additional information must always be given, ***unless*** this is ***obvious*** - which is stricter than the Directive - and in addition stipulates that the data subjects must be informed of the ***actual recipients*** of the data (rather than just the categories of recipients) and of the fact that the data are to be held in a (structured) **filing system** or **automatically processed**.

As far as the **timing** of the information is concerned, there are ***similar divergencies***. The laws in Belgium, Denmark, Greece, Luxembourg, the Netherlands, Italy and Spain all demand that the information be provided "***when the data are collected***", or "***before the data are provided [by the data subject to the controller]***", or "***beforehand***" or "***at the latest when the data are obtained***" - while the laws in Austria, France (both current and proposed), Germany and the UK, and the proposed new (amended) law in Ireland, are **silent** on the issue, and the laws in Finland and Sweden ambiguous. However, the UK data protection authority has advised that:

> "As the [UK data protection law] makes no specific provision relating to timescale in the case of data obtained from data subjects, it should be ***presumed*** that the fair processing information must be provided to the data subject **at the time that the data are obtained**."

The data protection authority in Ireland is likely to take the same view. In Denmark too the authorities agree that the information must be provided as soon as practicable and, if the data are collected by means of a **form**, they would also recommend that the information be

[68] Note that the first two matters (information about the identity of the controller and his representative, and information about the purpose of the processing) are not yet listed in the current (pre-implementation) law, although the data protection authority already generally requires the provision of this information in most cases.

provided on that form. The latter is also formally required in Portugal and under the current law in France, as already noted.

8.2 informing when data are collected otherwise

Article 11
Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,
- the recipients or categories of recipients,
- the existence of the right of access to and the right to rectify the data concerning him -

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

The laws of the Member States also differ in respect of the information that must be provided to data subjects when data on them are obtained other than from the data subjects themselves. Again, some stay quite close to the Directive, some qualify the requirements of the Directive in terms seemingly at odds with the Directive, and yet others go beyond the requirements of that instrument.

Thus, the laws in Austria, Belgium, Denmark, the Netherlands, Portugal and Sweden all again basically follow the Directive by stipulating that the controller must inform the data subject of the **identity of the controller** and the **purposes of the processing**, and of **further information** only to the extent that that is ***necessary to ensure fair processing*** in respect of the data subject (or when this is necessary to allow the data subject to exercise his rights, or to safeguard those rights, as it is again put in the laws in Denmark and Sweden; or *unless* it is *not necessary* to ensure fair processing, as it is again put in the Belgian law). The law in Luxembourg again lists the same matters, but again without reference to "fairness" (although this must again be regarded as implied). The law in the UK also basically stipulates these matters - but then again qualifies this by adding that the information only needs to be

provided "***so far as practicable***" and that the data subject must either be provided with the information, or have it "***made readily available to him***".

The laws in Austria, the Netherlands and the UK again do not provide the examples of the kinds of additional information that may need to be given, set out in the Directive, while the first of these does give examples of the kinds of **situations** in which fairness may require the providing of additional information (as already mentioned). However, as noted in the previous sub-section, in the UK, the question should (according to the Data Protection Authority) again be answered by reference to what the data subject can **reasonably foresee** or understand from the information that is provided as to the purposes and consequences of the processing of which he is informed, and of any disclosures this may involve. In the Netherlands, the Explanatory Memorandum to the law again provides clarification, including the following example.

> CASE EXAMPLE: In the Netherlands, if data are collected by means of ***data matching*** or ***linking of databases*** (NL: *koppeling*) - which is regarded as posing special risks to data subjects - the data subjects must be informed of this, with a description of the kinds of databases that have been linked and an indication of how the data subject can exercise his rights of access and correction with regard to the "matched" data.

By contrast, the laws in Finland, Greece, Italy and Spain, and the propos ed new (amended) law in France, are again more demanding, in the same way as discussed in the previous sub-section, by requiring that **all the information** be ***always*** provided.[69] Several of them also require that the information should (in principle) be given ***in writing*** (Greece, Italy) or at least "***explicitly, precisely and unequivocally***" (Spain). The proposed new (amended) law in Ireland on the one hand goes beyond the minimum requirements of the Directive in this respect, by stipulating that (in addition to information on the identity of the controller, and the purpose or purposes of the processing) data subjects must also be informed of the **categories of data** concerned and the **name of the original controller** (as well of *other information* insofar as necessary to ensure fair processing) - but on the other hand that proposed law again adds the dubious qualification (derived from the UK law) that the other the information only needs to be provided "***[in]so far as practicable***" and that the data subject must be provided with the information, or have it "***made readily available to him***".

There are also differences with regard to the **timing** of the information. Most States - Belgium, Denmark, Finland, Italy, Luxembourg, the Netherlands, Sweden and the UK - basically follow the Directive by stipulating that the information must be provided at the time of first recording of the data or, if disclosure is intended, at the time of the first disclosure. The same is done in the proposed new (amended) laws in France and Ireland.. However, the law in the UK adds usefully that the postponement in the latter case is only acceptable if the disclosure takes place "within a reasonable time" (without clarifying this further). It may be noted that the UK data protection authority feels that the rules in the Directive about when the information is to be provided make **no sense** (and that the addition about the data having to be provided "within a reasonable time" does not suffice to overcome this):

> "The requirement is that where data have not been obtained from the data subject he/she is provided with information 'at the time of undertaking the recording of personal data or

[69] In France, this is the more significant, since the current (pre-implementation) law does not contain any specific provisions requiring the informing of dat subjects in these circumstances.

> if disclosure to a third party is envisaged, no later than the time when the data are first disclosed'. In specifying this level of detail the Directive imposes a requirement that makes no obvious sense. If a data controller records personal data but does not intend to disclose the data it must inform the data subject straight away. If it records the data with the intention that they will be disclosed at some point, a situation which is more likely to have a significant impact on the data subject it can delay providing the information until the time of disclosure however distant this might be. (The UK law has sensibly imposed a requirement that this is 'within a reasonable period' but the basic problem remains)."

In Denmark, the data protection authority, as a rule of thumb, regards a delay of no more than **10 days** as acceptable.

The law is Austria is somewhat ambiguous in that it stipulates that the information must be provided "in connection with" (*im Anlass*) the data collecting (but this is in addition to the stipulations about the "revealing" of the controller's identity in "messages" to the data subject, noted in the previous sub-section). The Greek law requires that the informing be done when the data are collected (i.e. in the very collecting stage), without allowing for a delay if disclosure is intended; while the Spanish law stipulates that the information must be provided (irrespective of whether a disclosure is intended) within **three months** - which may be too lax in terms of the Directive.

9. rights of data subjects [Arts. 12, 14 & 15]

introduction

The data subject rights are central to data protection: they are the primary means to assert one's "right to informational self-determination". The Directive provides both for the **traditional rights**, already contained in earlier international data protection instruments (the right to obtain, on request, ***confirmation*** of whether data on one are being processed; the right to be given ***access*** to [i.e. a ***copy*** of] the data [in intelligible form]; the right to have incorrect or outdated data ***corrected, updated or erased***; and the right to ***object to direct marketing use*** of one's data). But it also adds **new rights**: a ***general right to object***; a special right not to be subject to a ***fully automated decision based on an "evaluation" of one's "personal aspects"***; and the right to be informed, on request, of the "***logic***" used in such decisions.

summary of findings

The study found that all the Member States grant data subjects the right to obtain **confirmation** of whether data on them are being processed (although two only imply this).

With regard to the right of **access**, there are ***some differences*** concerning the extent to which information must be provided on ***sources*** or ***other persons***, concerning the providing of a ***hard copy*** of the data, and concerning the providing of information on the "***logic***" used in certain decisions (with some Member States extending the latter right to other decisions than the kinds referred to in the Directive).

Some Member States provide some useful ***clarification*** on what is the "**appropriate**" remedial action concerning various forms of wrongful processing, while others are (like the Directive) more general in their wording.

There are ***quite significant differences*** as concerns the **general right to object**: some Member States extend this right to ***all (or most) processing***, while others do not provide for this right at all.

As far as the **right to object to direct marketing use of one's data** is concerned, there are again ***considerable differences***. First of all, several Member States extend this right to other matters, such as ***market research*** and ***opinion polls*** (which is both contrary to the Directive and causes problems in

trying to distinguish these activities from other [statistical or social] research). Ans as to the details, and specific procedures, surrounding this right, the laws differ between themselves and fail to clearly fall within one or the other of the two alternatives offered by the Directive.

There are also ***significant differences*** in the ways in which the Member States apply the **right not to be subject to fully automated decisions in which a persons "personal aspects" are "evaluated"** - with some giving this right a much wider scope (on paper) than others. In practice, however, the application of this right is ***rare***.

matters to be further clarified or addressed

The **considerable differences** in the rights accorded to data subjects in the different Member States will be most notable with regard to ***transnational activities***, since these rights too depend on the "applicable law" (even if the enforcement of these rights may be in the hands of the data protection authority of the country where the data subject is based). This is not conducive to the Internal Market.

There are also still many areas in which the exact scope and meaning of these rights remains unclear - although some Member States do provide useful clarification on specific points. Again, it would be useful if such clarification (based on such already-provided guidance) could be issued at a European level.

- o – O – o -

9. rights of data subjects – detailed findings

9.1 right of access

Article 12
Right of access

Member States shall guarantee every data right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred .to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

The laws in all the Member States provide for the right of data subjects to receive **confirmation**, on request, of whether data on them are processed by a particular controller - although in Austria and Germany this is ***implied*** in the right of access rather than specifically stipulated, while conversely the law in Finland adds expressly that if controllers do *not* process data on the data subject they must inform him of that, while the law in Greece (more significantly) extends the right to confirmation about whether data ***have been processed*** on the data subject in the past.

The laws all also provide for the **right of access** to the data - but there is some ***lack of clarity about its general scope***; and there are ***some differences*** on certain specific matters. On the general question, concern has been expressed by controllers in several countries (in both the public and the private sector) that the law would require them to carry out **exhaustive searches** for ***any data*** on the person seeking access which ***might*** be held somewhere, ***anywhere***, on their systems. For major organisations, this would be enormously costly. Little formal guidance has as yet been provided in this respect, but **informally** ***the data protection authorities tend to accept that controllers are, in ordinary cases, not required to carry out searches in response to an access request which they would not carry out themselves in the course of their normal, day-to-day operations***. If the controller can retrieve the information for his own purposes, he should retrieve it in response to an access request; data which would not normally be retrievable need not normally be provided. This would only be different if

there was some special reason to look for other, "hidden" information, e.g. if the data subject has shown (or if it would *prima facie* appear) that data originated from the controller in question and was passed on to others, more in particular if the passed-on data were incorrect or had been disclosed in contravention of the law. Of course, this "rule of thumb" should not be abused. For instance, organisations are increasingly confronted with request from data subjects (e.g. disgruntled former employees or dissatisfied customers) for copies of all emails in which comments are made about them. It may be awkward - and may even expose an organisation to liability - to provide such copies. But if they were sent, and are retained and accessible by reference to the data subject, they should be disclosed. Similarly, access may not be denied or limited on the grounds that providing full access might reveal **commercially sensitive information**:

> CASE EXAMPLE: The data protection authority in Ireland examined a case in which a **credit reference agency** had provided a complainant seeking full access to all the data held on him with a summary of the data only. The agency argued that printing off a copy of the information which they held on computer would identify the software package they used, and that this was commercially sensitive information. In response, the Commissioner's office "pointed out that the company was free to take any reasonable steps to hide the identity of the software package. However, the individual had a clear legal right to see a copy of all the information relating to him." The company agreed to provide a full copy to the data subject.

Clearly, these are matters on which more such formal guidance - prefereably at the European level - is urgently called for.

The most important **formal difference** in the laws is that some countries - Greece, Spain and Sweden - require controllers always to inform data subjects, on request, of the **sources** of the data - and not just of "***any available information***" as to these source[s]. The law in the Netherlands stipulates that if the data to which access is sought contain **data on others** (including sources), the controller must ***contact*** those others and must decide whether to disclose the information in the light of the response of the other person. The law in the UK contains a similar provision, according to which information about other individuals must be disclosed to the data subject if the other person ***consented*** to this, or if it is "***reasonable***" in the circumstances to provide the data without such consent. However, that law also contains a further (full) exemption concerning **references given in confidence** to the controller for the purposes of, *inter alia*, education, training or employment. The UK data protection authority herself has pointed out that this "blanket exemption" has "[no] clear foundation" in the Directive. The current (pre-implementation) law in Ireland still contains an even wider exemption, according to which **controllers may refuse** to disclose any information relating to another individual, unless that other person ***consented*** to the disclosure (although controllers are obliged to disclose as much information as possible which does not identify that other person). This also applies to information on another person which identifies that other person as the ***source*** of the data on the data subject making the access request. The proposed new law in that country is likely to amend this exemption to some extent. The current draft stipulates that the exemption will not apply if the data on the other person consists of an ***expression of opinion*** (by that other person) about the data subject seeking access to the data. Consideration is also being given to not exempting information concerning another person, if

it relates to that other person's "normal duties". Both suggestions however still fall short of the Directive.[70]

In Germany, the right of access is ***extended*** by the data protection law to data held in non-structured files, if the controller processes the data "professionally" for the purpose of providing the data to others (e.g. if he is a credit reference- or detective agency); in other countries such extensions flow from the special rules relating to such specific kinds of companies. The Austrian law adds that data subjects must also, on request, be provided with the identity of any ***processors*** who have processed the data on behalf of the controller, while the Greek law adds that the controller should specifically inform the data subject of any ***developments*** in the processing since the last access request.

All the Member States except Spain in principle give data subjects the right to obtain a **copy** of the data (although the Danish law refers to the data subjects being provided with information "on" or "about" their data, the law is in fact applied so as to require a the provision of a copy of the data there too). In Austria, Finland and the UK, the law expressly mentions that **if the data subject agrees**, the controller can, alternatively, offer the data subject **access** (e.g. on the controller's premises, or on-line) ***rather than a hard copy*** of the data. The Spanish law provides for this alternative too, but ***without stipulating that if the data subject wants he can demand a hard copy rather than mere access***. The proposed new (amended) Irish law also allows for the provision of information other than in "permanent form" if the data subject ***agrees*** to this, but also allows for this if "the supply of [a copy in permanent form] is ***not possible*** or would involve a ***disproportionate effort***". In France, access to data on ***criminal convictions***, ***"penalty points"*** on a driving licence, and certain ***medical data*** is provided by allowing the data subject to inspect the data, but without providing a hard copy, so as to frustrate attempts at so-called "**enforced subject access**" (in which a person is pressurised into using his right of access to such data, and to submit those data to another person - e.g., a prospective employer).

The laws in all the Member States give data subjects the right to be provided, on request, with information about the "**logic**" used in processing operations which involve the taking of fully automated decisions on the based on a personality "profile" (although they sometimes use somewhat different terms in this respect, such as "rules" or "operating principles" or "reasoning") - but three Member States - Greece, Italy and the Netherlands - extend this right to ***all kinds of automated decisions***, i.e. not just the ones involving an "evaluation" of a person's "personal aspects". The proposed new (amended) law in France extends the right to information about the "logic" which formed the basis of "***any automated processing, the results of which were against [the data subject]***" (as long as the information does not infringe **copyright**); and the proposed new (amended) law in Ireland will extend the right to information about the "logic" used in any processing by automatic means of data on the data subject, if this processing "**has constituted *or is likely to constitute* the sole basis for any decision significantly affecting him or her**". One Member State - Portugal - even extends it to the logic involved in ***any automatic processing of data*** concerning the data subject. The Luxembourg law says that the right applies "***at least***" in the case of fully automated, "significant" decisions of the kind further discussed below, at 9.4. While this wording derives from the Directive, that instrument merely intended to give the Member States discretion in

[70] Note that the Irish Freedom of Information Act applies a different exemption, under which individuals may be denied access to information in official documents which is provided in confidence. On the "delicate" relationship between the data protection law and the FOI law, see below, at 10.2.

the matter. Merely repeating the words leaves the law unduly vague. These extension are significant, given that the provision in the Directive on such decisions applies to a very limited range of decisions only (as also discussed below, at 9.4).

The Austrian law stipulates that the data subject may be asked to ***assist*** in searching for his data (for instance, s\he may be asked to clarify whether s\he was a customer or a member of the organisation concerned, and if so when), and that once a subject access request has been made, the data concerning that person may not be ***destroyed*** for four months (i.e. while the request is being processed). However, the UK data protection authority advises controllers differently:

> "The information given in response to a subject access request should be all [the personal data][71] at the time the request was received. However, **routine amendments and deletions of the data may continue** between the date of the request and the date of the reply. To this extent, the information revealed to the data subject may differ from the data which were held at the time the request was received, even to the extent that data are no longer held. But, having received a request, the data controller must not make any special amendment or deletion which would not otherwise have been made. The information must not be tampered with in order to make it acceptable to the data subject."

The German law stipulates equally usefully that if a data subject approaches an entity which is part of a **complex organisation or groups of organisations** (such as a group of companies), the entity (e.g. a daughter company or branch or department) which is approached must ***pass on*** the access request to other parts of the group as appropriate.

All the laws provide for the right of **rectification or erasure** and all except the Finnish law (but including the proposed new (amended) Irish law) also expressly refer to "**blocking**" in this regard (with some of them indeed adding a specific definition of the concept, as noted above, at 2.9). In Greece, the right to corrective action is formulated in very general terms in the context of the "right to object" - which means that it applies to all contested processing (as further discussed below, at 9.2). The law in Belgium is more specific about what remedial action is "appropriate" in respect of erroneous processing, in that it clarifies that data subjects have the the **right to have data rectified** if they are ***incorrect***; and **erased or blocked** if they are ***incomplete, irrelevant, held for longer than necessary in view of the purpose of the processing, or if the processing is otherwise contrary to the Law***. The same clarification is also added in the Explanatory Memorandum to the Dutch law. The Austrian and German laws add clarification to the effect that documents retained for historical purposes or "documentation" need not be rectified but that data subjects have the right to have their comments added to the record. The Austrian law also adds clarification about regularly issued compilations of data (such as address lists, or membership directories), which should be corrected at the next regular issue.

The German and to some extent the UK law focus on the action that should be taken if **disputes** arise, rather than on the prior matter of rectification by the controller in response to a request for such action (although of course in both countries that is the normal process). As

[71] The law literally refers to "all [the information] which is contained in the personal data", but this is merely the result of the rather cumbersome terminology in the law, which distinguished between "information" and "data" in a way which is not the case anywhere else, as noted above, at 2.1.

far as such disputes are concerned, it may be recalled that under the UK and Irish laws data are only regarded as inaccurate if they are "incorrect or misleading as to any matter of ***fact***".

9.2 the general right to object

Article 14
The data subject's right to object

> Member States shall grant the data subject the right:
>
> (a) at least in the cases referred to in Article 7 (e) and (f),[72] to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.

The general "**right to object**" to processing on "***legitimate grounds***" originates in France: it was included in the current (pre-implementation) law in that country (adopted in 1978) through a Parliamentary amendment. Prior to the Directive, it was however not widely adopted elsewhere - or at least not in those terms: the possibility of challenging processing operations with which a data subject disagreed was of course often possible, on a variety of legal grounds, some of which were so wide as to be tantamount to a "general right to object" (e.g. objections to processing in the public sector based on broad general principles of administrative law, or challenges to processing in the private sector on the basis of broad civil-legal principles such as *faut*, *unerlaubte Handlung* or *onrechtmatige daad*.

Following implementation of the Directive, most of the laws in the Member States now do include this right - but they apply it **quite differently** in these laws. Thus, the laws in the Netherlands, Portugal and the UK apply the right strictly to the minimum required by the Directive: processing for tasks carried out in the **public interest** or in the exercise of **official authority** [Art. 7(e) of the Directive] and processing on the basis of the "**balance**" criterion [Art. 7(f) of the Directive] (the UK law allows the Lord Chancellor to extend this right to processing other bases, but this has not been done). The proposed new (amended) Irish law also limits the right to processing on the basis of these two criteria only. Indeed, the UK law and the proposed new (amended) Irish law add that the right can be exercised only on the ground that, for specified reasons, the processing causes (or is likely to cause) "***substantial***

---

[72] As noted above, at 5, Art. 7 stipulates that all processing of personal data must be based on one of the following "criteria" (or grounds for lawful processing):

(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out 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; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

damage or substantial distress" to the data subject or another person which is "***unwarranted***". In other words, under these laws, an objection is only to be regarded as "***justified***" if such "substantial, unwarranted" effects are likely.

The law in Germany provides for the right in two separate provisions, one concerning procesing in the **private sector** on the basis of the "***balance***" criterion, and another one concerning processing by **public authorities** for tasks carried out in the ***public interest*** or in the exercise of ***official authority*** - but between them these too will generally cover the minimum requirements of the Directive.

The other laws either do not provide for this right, or limit it contrary to the Directive - or they extend it to processing on the basis of more (or indeed any) criteria.

Specifically, the laws in Denmark and Italy stipulate the right in completely general terms, to apply to **all processing**; the law in Austria applies the right to **all processing** except processing necessary to comply with a ***legal obligation***; the law in Luxembourg applies it to all processing except when "***a legal provision expressly prescribes the processing***"; and the law in Belgium to **all processing** except processing necesary to fulfil a ***contract*** or ***pre-contract***, and processing necesary to fulfil a ***legal obligation***. As already noted above, at 9.1, the Greek law somewhat confuses the right to object with the right to obtain rectification, erasure or blocking of data - but would still appear to apply to **all processing**, and not just to processing which is contrary to the law.

The current (pre-implementation) French law exempts processing specifically indicated in the "regulations" governing processing in the public sector. It was already determined under that law that this did not exempt all such processing, but rather only processing which was excluded from the right to object in a ***specific provision*** to that effect in such a regulation. In the proposed new (amended) law this narrow interpretation of the exception (i.e. the wider application of the right) is expressly confirmed.

By contrast, the laws in Finland, Spain and Sweden do NOT contain provide for a **general right to object** - or at least not explicitly (the Swedish law applies the right to processing on the basis of **consent**, in the sense that it allows the revoking of consent at any time - but the same applies elsewhere). As far as Spain is concerned, the absence of the general right to object can be explained by the fact that the two citeria to which it must relate according to the Directive are severely restricted in the law in the first place, as discussed above, at 4, under the heading *the data protection criteria*. In particular, the criterion relating to processing in connection with a **public task** or with the exercise of **official authority** is, in the Spanish law, applicable only to ***public authorities*** - and any actions by such authorities (including any processing relating to such actions) can in any case be ***challenged*** (read: objected to) in ordinary ***administrative-legal proceedings***; while the application of the "**balance**" criterion is under that law limited to the processing of data derived from ***certain specific public sources*** (the population register, telephone directories, professional directories, newspapers, etc.) - and the use of data from such sources is subject to various requirements which enable persons listed in such sources to ***object*** to the use of those data, as further discussed below, at 9.3.

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: it will be difficult to show "compelling" reasons to object to processing which is necessary for the fulfilment of a

contract, or for compliance with a legal obligation, or to protect the "vital interests" of the data subject - and such objections may therefore be hard to "justify". The question of whether an "objection" is justified to processing based on the data subject's own previously given (valid) consent is better addressed in terms of the revokation of such consent (and the consequences of such a revokation). However, the restrictions of the right in the laws in Finland and Sweden (and to a lesser extent Spain) cause more significant difficulties in terms of the Directive.

9.3 the right to object to direct marketing use of one's data[73]

> ALTERNATIVE ONE:
>
> "Member States shall grant the data subject the right ... to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing. Member States [which opt for this alternative] shall take the necessary measures to ensure that data subjects are aware of the existence of [this right]."
>
> (Art. 14, first sub-paragraph of paragraph (b) and final sentence)
>
> ALTERNATIVE TWO:
>
> "Member States shall grant the data subject the right ... to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses."
>
> (Art. 14(b), second sub-paragraph)

As noted above, the Directive requires Member States to grant data subjects the **right to object** to the ***processing*** (or at least to the ***disclosure or use***) of their data for **direct marketing purposes**; and gives the Member States ***two options*** in this respect, i.e. the Directive offers the Member States two alternative ways of implementing this right. I have analysed this provision, and the (suprisingly different) requirements of the Directive with regard to these different options, in my Report on the Directives, prepared for the European and American direct marketing associations (FEDMA and the DMA-USA). An extract containing the relevant sub-section (included in section 6.i of that report) is attached.

The situation in the Member States is in fact further complicated. First of all, five of the Member States - Finland, Germany, Italy and Spain - extend the right to object to the use of one's data for ***direct marketing*** to the use of those data for ***market research*** and ***opinion polls*** (and in the case of Portugal even to all research), even though in practice (and in the relevant

---

[73] The discussion in this section is basically 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 subject to special Directives which are outside the scope of this study. Suffice it to note that with regard to ***telemarketing***, the relevant Directive provides for certain ***options*** - which ensures that the laws in the Member States differ, even leaving aside divergencies resulting from different interpretations (e.g., as to how to apply the law to "sole traders" who are acting as a commercial entity but are also "physical persons"). As far as marketing in the ***Internet*** is concerned, the rules are in flux, as a result of the adoption of a new *e*-Commerce Directive, which tightens the restrictions under the Telecommunications Data Protection Directive, but which has not yet been implemented. For details of the current situation in the Member States, see the country sections in D Korff, Report on the Directives, FEDMA\DMA-USA, 2002; cf. also the chapter in that book on *applying the rules on "applicable law" to the Internet*.

international codes, such as the ICC codes) a **fundamental distinction** is made between the two activities, with the relevant rules emphasising that for **direct marketing** ***personal (i.e. identifiable) data*** are (and must be) used, while **market research** relies on ***anonymised*** (or at least ***pseudonymised***) ***data***.[74] The extension of the right to object to dm-use of one's data to the use of one's data for such other purposes not only causes problems for **market research** companies, but also begs the question of how one can distinguish the latter from ***scientific or statistical research*** - for the benefit of which the Directive contains various **relaxations** of its rules. Here, it must suffice to note that the distinction cannot relate simply to the question of whether or not the research is "***commercial***": these days, most scientific research has some commercial element or perspective.

As far as the choice between the **two alternatives** is concerned, the dividing line is again not ***sharp***. The **first alternative option** (granting data subjects a right to object to dm-use of their data and ensuring general publicity for this) is clearly chosen in just four countries: Austria (under separate legislation), the Netherlands, Ireland (under the current (pre-implementation) law, which in this respect is not to be amended) and the UK. However, in the UK (in the words of the Data Protection Authority) the law "conspicuously fails" to ensure the general publicity which is to be given to the existence of this right: the direct marketing industry provides this publicity, but purely on a voluntary basis. The same applies in Ireland under the current law; nor are there any provisions in the proposed amendments to the current law which would remedy that omission.[75] The Luxembourg law also sets out the general right of each data subject "to oppose, on request and free of charge" processing of his or her data for dm-purposes; and the law adds that "the controller is obliged to make the existence of this right know to the data subject" - but as will be noted below, this stipulation is, in that law, ***in addition*** to a provision incorporating the second alternative means of implementing the right.

The law in Belgium also seems to provide for the **first alternative** - but a separate Royal Decree has added further duties, including a duty on the part of controllers to **offer** the right, which ***in effect*** means that in that country the ***second alternative*** option is now followed. The law in the Netherlands too has been tightened, although not quite to the extent required by the second alternative, in that ***direct marketing messages*** must contain **information** about the right to object to (further) dm-use of one's data.

---

[74] See also the specific **definition** of "***direct marketing***" in the UK law: "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals." Note that this is the traditional distinction. Recent developments, including in particular the establishment of large-scale "**data mines**", have the potential to erode this distiction, but the international trade associations stress the need to separate identifiable data used for direct marketing from anonymous (or at least encoded) data, even within such databases.

[75] The debate in Ireland is mainly focussed on the question of whether the general criterion of "***explicit consent***" for the processing of any data (i.e. also for non-sensitive data: see above, at 6.2) requires controllers to use an "***opt-in***" for dm-use of data collected for other purposes (rather than an "*opt-out*"). This somewhat fails to address the question of when processing for dm-purposes requires consent, and when it can be based on the (alternative) "balance" criterion. The data protection Commissioner has touched on the issue in his advice on matters to be addressed in codes of conduct, noted with reference to the question of "consent" above, at 6.2 (codes are also further discussed below, at 15), but has for now deliberately left the matter somewhat open by merely saying that "*In determining which of these options is applicable* [i.e. implicit consent to obvious, primary purposes; additional 'opt-in' consent; 'opt-out' consent; and processing on the basis that the data subject was informed but did not object], *a data controller will need to have regard to the European Union's Data Protection Directive's requirement of 'unambiguous consent', on the one hand, and the interplay with the alternative basis of a 'legitimate interest', which does not interfere unduly with the fundamental right to privacy* [i.e. the 'balance criterion'], *on the other hand*."

The **second alternative option** (under which data subjects must be specifically ***offered*** the right to object to dm-use of their data) is similarly clearly chosen by five countries only: by Belgium (as already noted, following the Royal Decree), by Denmark (which however applies the rules in question only to ***companies*** [DK: *virksomheder e.v.*] and to data on ***consumers***), and by Italy, Luxembourg and Spain. However (as just noted), in the Luxembourg law, this second alternative of the right is set out separately from, and in addition to, the right under the first alternative. In other words, the Luxembourg law requires compliance with **both alternatives**, ***cumulatively***. By contrast, the Portugese law lists **both alternatives *as alternatives*** - which suggests that controllers can choose which alternative they want to comply with. The rules in five further countries - Finland, France(already under the current law), Germany, Greece and Sweden - ***in effect*** get 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 (or at least be informed of it and of the means that can be used to exercise it, which basically amounts to the same thing). However, the law in Finland is somewhat more lax as concerns the use of "***campaign files***" which are kept for a relatively short period, and for one-time use in a single marketing campaign only. And in Germany, the rules that apply to the collecting of data from sources other than the data subject fall short, not just of the second, but also of the first option, in that they do not ensure that data subjects are aware of this right in those cirucmstances.

As far as the **mechanisms** for ensuring compliance with the right is concerned, it must be noted that special services have been established to this end in all the Member States *except* Luxembourg. These services - usually referred to as "**Mailing Preference Services**" (MPSs) or "***Robinson Lists***" - maintain **suppression lists** to which individuals (sometimes only ***consumers***) can have their details added. Companies sending out direct marketing messages (mailings) "clean" their final mailing lists against these centrally provided suppression lists and ***exclude the "objectors"*** from this final list.[76] This ensures that these individuals do not receive the mailing in question - but of course it does not mean that their data are "***erased***" from all the files in question (which would make it more difficult to ensure that they will be excluded from subsequent mailings too). In most countries, the relevant Data Protection Authority accepts that, in principle, use by industry of the relevant MPS will suffice to comply with the right in the Directive, but in some countries (e.g., Spain) it is clear - and made clear in the relevant rules (in Spain, in a detailed *Instruction* on the exercise of data subject rights) - that if a data subject insists, he or she can demand that his or her data are actually removed from the files in question. The MPS- or "Robinson"-services are also arranged in different ways. They are operated by **industry** on a self-regulatory basis in Austria, Belgium, France, Finland, Germany, Ireland, Italy, the Netherlands, Portugal, Spain and the UK, but by **public bodies** in Denmark, Greece and Sweden.

The picture is therefore overall still **quite confusing** and not at all conducive to opening the European market to cross-border direct marketing campaigns or to pan-European market research.

ATTACHED: Extract from D Korff, Report on the Directives, FEDMA\DMA-USA, 2002.

[76] Separate **Fax- and Telephone Preference Services** have also been established in several countries, and an **e-MPS** has been created for the Internet, but these relate to the more specific rights under the Telecommunications Data Protection Directive and will therefore again not be discussed here. For details, see the website of FEDMA (the Federation of European Direct Marketing): http://www.fedma.org/.

ATTACHMENT TO SECTION 9.3 (the right to object to dm-use of one's data): Extract from D Korff, Report on the Directives, FEDMA\DMA-USA, 2002:

the specific right to object to direct marketing use of one's data:

The framework Directive adds to the general but qualified right to object a more specific but unconditional right to object to the processing of one's data for **direct marketing** purposes (Art. 14(b)). Since this report is aimed, in particular, at the direct marketing sector, this rather convoluted provision (the result of a political compromise) deserves some special attention. However, it must also be noted that some other, closely related rights, are contained in the telecommunications data protection Directive, as discussed separately below, at ii. The overall implications of these different provisions in those different directives are discussed below, at iv.

According to Art. 14 (b) Member States must grant each data subject the right:

"to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosure or uses."

To this, the Directive adds, in a final clause:

"Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b)."

Article 14 therefore offers the Member States a choice of **two alternative systems**:

ALTERNATIVE ONE: According to this first alternative, the State must grant all data subjects "**the right to object, on request**" (as well as free of charge) to "the **processing** of personal data relating to him which the controller anticipates being used for the purposes of direct marketing" - whereby **the State** must "take the necessary measure to ensure that data subjects are aware of the existence of [this right]"

ALTERNATIVE TWO: According to this second alternative, the State must grant all data subjects "**the right to be informed**, before personal data are disclosed for the first time to third parties or used on their behalf for the purpose of direct marketing, and to be **expressly offered the right to object** free of charge to **such disclosures or uses**."

Although the framework Directive speaks of a right to "object to" - rather than a right to prevent or stop - the processing in question, it is clear that the latter is intended. If a data subject exercises the right to object to direct marketing (in either variant), the controller(s) in question must comply with that objection. To state this in terms compatible with the general right laid down in Art. 14(a) (with regard to which the right contained in Art. 14(b) is a lex specialis): such objections are always to be regarded as "justified". However, as we shall see, one can perhaps argue about how such objections are to be complied with.

With regard to both alternatives, we should distinguish between the scope and substance of the rights mentioned, and the conditions attached to these rights. As we shall see, the alternatives provided for in Article 14 of the framework Directive differ in both respects.

the (alternative) requirements of the framework Directive concerning the scope and substance of the right to object to direct marketing use of one's data:

It is notable, if somewhat surprising, that the alternative arrangements envisaged in Art. 14(b) of the Directive relate to rights with quite different scope and substance: the first alternative provides for a right to object quite generally to the **processing** of one's personal data for direct marketing purposes, while the second alternative stipulates a right to object to the **disclosure** of one's personal data, as well as to the **use** of one's data by the controller **on behalf of a third party**, for direct marketing purposes (such as, in particular, in "host mailings").

"Processing" clearly encompasses much more than just the disclosure of personal data and the use of data on behalf of a third party: it includes not just the collection of data, but also their disclosure, analysis or use (cf. Art. 2(b), discussed above, at 2.i). The right provided for in the first alternative option is therefore, on paper, much wider than the right provided for in the second alternative option: in Member States which opt for the first alternative, data subjects must (if the text of the Directive is to be applied fully) be granted a right to object to the collection of personal data by the controller in question for direct marketing purposes (also, e.g. from other sources than the data subject, such as public registers), to the analysis of the data by that controller for direct marketing purposes (e.g., in "profiling"),[77] to the use of the data by the controller for his own direct marketing purposes (i.e. for the mailing of his own customers) - as well as to the disclosure to and\or use on behalf of a third party, for direct marketing purposes.

By contrast, the right provided for in the second alternative option is (on paper) limited to the latter two forms of processing: to the disclosure of the data subject's data to third parties and to the use of those data on behalf of such third parties. However, data subjects in countries which opt for this second alternative of course still retain the general right to object to the other forms of processing: to the use by a company of its own direct marketing to its own customers, or to the use of (identifiable) customer data for analysis or "profiling" (and to the anonymising of their data to that end). It is difficult to see how objections to such uses of a data subject's data will ever be regarded as not "justified". Indeed, to the extent that any such processing is based on the "balance" condition, the raising of such an objection would undoubtedly tilt the balance against the controller; and to the extent that it is based on "consent", data subjects are entitled to withhold that, or revoke it. Data subjects in countries which opt for the second alternative are therefore in practice likely equally to enjoy the right to object to direct marketing by companies of which they are a customer; and they are also likely to be allowed to oppose the use of their personal data in "profiling", or the anonymisation of their data for (market) research purposes.

Whether these issues will make much difference remains to be seen. In practice, under the old laws of the Member States, data subject rights in respect of direct marketing were generally deemed to have been respected as long as the names and addresses of objectors were **suppressed** from (final) mailing lists. In spite of stricter formulations in several laws, on the lines of the terms used in the first alternative option of Art. 14(b), the data protection authorities acting under those old laws generally accepted that suppression (rather than an end to all direct marketing-related processing, including disclosures) sufficed.[78] It is likely

[77] In principle, data subjects can only object to processing of their data for as long as these are "personal data", i.e. for as long as they can still be linked to them. They cannot object to the processing of anonymised data. However, as discussed above, at 2.*i*, the actual act of anonymising data is a form of processing - and data subjects can therefore also object to this.

[78] For a summary of the situation under the previous laws of the Member States in this regard, see D. Korff, o.c. (*supra*, footnote 24), pp. 34 – 37.

that they will continue to do so in countries which opt for that alternative (one Government - the Dutch one - made this clear even before adopting a new law). But it remains a fact that that view of the right as stipulated in the first alternative option under Art. 14(b) is at variance with the clear, literal meaning of the text of the Directive. It is possible that - in spite of this conflict between the letter of the Directive and the approach of the authorities (and industry) - the Member States will by and large adopt the first alternative option in their laws, but will continue to accept the current practice of suppression of names from the final mailing lists only. However, it is also not impossible that at some stage the courts - and the Court of Justice - are asked to rule on this matter. If and when that happens, that practice might be found to contravene Art. 14(b), first option.

the (alternative) conditions attached to the right to object to direct marketing use of one's data:

The Directive also lays down different conditions under which the right to object to direct marketing use of one's data is to be exercised - although again, these are perhaps not as far removed from each other as might appear. The right as provided for in the first alternative option, is to be exercised "on request" - but Member States choosing that option are required to take "the necessary measures" to ensure that data subjects are aware of the existence of that right. In practice, this can be done by the State approving measures taken by the direct marketing industry to publicise the existence of the right widely - in particular, through regular general advertising campaigns (paid for by the industry) promoting the Mailing-, Fax- and Telephone Preference Services (as further discussed below, at v).

By contrast, the right provided for in the second option is to be "expressly offered" to the data subjects by the controller - presumably, in the course of the former being "informed" by the latter of the intended disclosure or use or behalf of the data (which must be before the data are disclosed or used on behalf of third parties for the first time).

Once again, the differences may be less stark than they might appear. In particular, even in countries which opt for the first alternative in Art. 14(b), controllers will normally nevertheless have a duty to inform data subjects of an intention to disclose their data for direct marketing purposes - and indeed, if they want to do so on the basis of the "balance" provision (Art. 7(f)), they may still need to (at least) offer an "opt out" from such disclosures before they take place (see above, at 5.iii). If they require the consent of the data subjects - e.g. if the data are sensitive, or if the processing can significantly affect the data subjects - this too will entail at least the informing of the data subjects, clarification that the granting of such consent is voluntary, and an indication by the data subjects that they agree to the "specified" use of their data (idem).

9.4 the right not to be subject to a fully automated decision

Article 15
Automated individual decisions

> 1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
>
> 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
>
> (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
>
> (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

The above provision in the Directive stems from certain rules in the current (pre-implementation) French law - expanded on in the proposed new (amended) law in that country, as noted below - which reflect the injunction in the law (noted above, at 1) that **information technology must serve mankind** and **should not violate "human identity" or fundamental rights** and which therefore prohibit the taking of ***judicial, administrative and private-sector decisions*** on the basis (or the sole basis) of ***automated processing*** of data which constitute a "***personality profile***".

Following implementation of the Directive, the laws in all the Member States which have implemented the Directive now contain provisions on the lines of the one in the Directive, quoted above - but again with some **significant differences**. Thus, the laws in Austria, Belgium, Germany, Finland, the Netherlands, Portugal and Sweden, as well as the proposed new (amended) law in Ireland, set out the **in-principle prohibition** on the taking of the kinds of decisions mentioned, and the ***basic exceptions*** to this prohibition, in terms similar to the Directive. However the laws in Belgium and Sweden, and the proposed new law in Ireland, apply the exception 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**. In other words, the legislator in these Member States felt that the offering of this possibility is also a sufficient safeguard in that other context. The proposed new (amended) Irish law also sets out a general exception to the in-principle prohibition on the taking of automated decisions, if the data subject ***consents*** to the processing - which presumably means that if someone consents to the taking of a fully automated decision of the kind covered by the law ***before*** the decision is made, s/he can no longer invoke the right to object afterwards.

The laws in Austria and Finland on the other hand allow for the taking of such decisions on the basis of any **law** - without specifying any ***safeguards*** (which is contrary to the Directive). In Portugal, the law does not contain the exception allowing for the taking of such decisions

on the basis of a law, but rather allows for such decisions (other than in a contractual context) only on the basis of a special **authorisation** issued by the data protection authority.

The German law adds the **clarification** that if there has been a negative decision of the kind mentioned, the data subject must be ***informed*** of this; and that if a data subject challenges such a decision, the controller is obliged to ***actually review*** that decision. The latter point is also made in the Explanatory Memorandum to the Dutch law.

The other laws and proposed new laws all **differ** more substantially from the Directive, and cannot be easily put together in one group.

Thus, the Greek Law gives any person the right, not just to "put his point of view" (i.e. to challenge) such a decision, but to "request from the competent court the **immediate suspension or non-application** of ***any act or decision*** affecting him, based solely on ***automated processing of data intended to evaluate his or her personality*** and especially his or her effectiveness at work, creditworthiness, reliability and general conduct." This right applies with regard to the taking of such decisions by administrative authorities, public law- or private law- entities or -associations and natural persons alike (*idem*). The right can be exercised "even when the other substantive conditions for provisional judicial protection" (i.e. for injunctions) do not apply, i.e. there does not have to be any illegality or impropriety involved in the decision. Nor does the Law require that the decision had legal or other "significant" effects: it suffices that the decision was a purely automated one and involved an "evaluation" of the data subject's personality or conduct. Presumably, if such a fully automated decision is suspended or dis-applied, the controller must replace the suspended or disapplied automated decision with a "human" one, i.e. the controller (or one of his employees) must review the decision in person. Apart from the extended scope of the right, this would bring the Law more or less in line with the Directive.

The Luxembourg law stipulates that individuals ***may be*** subjected to "**an individual automated decision which produces legal effects**", if the decision is taken in the course of entering into or performing a **contract** and if the request for the contract, made by the data subject was "***satisfied***" or if there were "***suitable measures to safeguard his legitimate interest, such as the possibility to put his point of view***", or if the decision "is ***authorised by a law*** which also lays down ***measures to safeguard the data subjects legitimate interests***." Apart from reversing the approach by stipulating when fully automated decision may be taken (rather than saying that data subjects have the right not to be subject to such decisions except in certain circumstances), the stipulation in the Luxembourg law also - and more importantly - refers to a **much broader category of decisions**: it does not say that the provision only applies to decisions "based solely on automated processing of data intended to evaluate certain personal aspects relating to [the data subject]", but applies to all "automated decisions" which "produce legal effects". The law not yet having come into force, there is of course as yet no practice to show how this much broader provision will be applied.

The proposed new (amended) law in France retains and builds on **two strict rules** in the current (pre-implementation) law which in fact, as noted above, inspired the provision in the Directive. The first rule says that **no decision in legal matters** (i.e. by courts, but also by the police, etc.) and which amounts to (*implique*) "***an assessment of the behaviour of a [natural] person***" may be "***based on automated processing of personal data aimed at evaluating certain aspects of [that person's] personality***". The second rule contains a similar

prohibition with regard to **administrative or private** (private-sector) **decisions with legal effect in respect of a [natural] person**, based solely on "***automated processing of data*** [note: not just personal data] ***aimed at defining the profile of the data subject***" or at "***evaluating certain aspects of his personality***". Next, the law sets out a **single exception**, with regard to decisions taken in the course of the entering into or the performance of a **contract**; the exception applies, provided that the data subject "***was given an opportunity to put forward his comments [on the decision]***." It should be noted that (other than in the Directive) this requirement applies even if "the request of the data subject for the entering into or performance of the contract" has been "satisfied"; and that the law the law does not envisage any other "suitable measures to safeguard [the data subject's] legitimate interests". Furthermore, the law does not allow for exceptions to the two prohibitions on the basis of a **law**: apart from the one exception concerning decisions concerning a contract, the prohibitions mentioned are ***absolute***.

The Spanish Law also contains **two provisions** on the taking of decisions based on "evaluations" of an individual's "personality". The first grants all (Spanish?) citizens the - it would appear, ***absolute*** - "**right not to be subject to** a ***decision which produces legal effects for them or which significantly affect them and which is based solely on processing of data intended to evaluate certain aspects of their personality***". The Law goes on to say, in a second provision, that data subjects have a **right to challenge** "administrative acts or private decisions which involve an ***assessment of [their]*** **behaviour**", if the only basis for this assessment is the processing of personal data on them which "provides a ***definition of [their] characteristics or personality***." In this latter case, the data subject has the right to obtain **information** on the ***assessment criteria*** and on the (computer) ***programme*** used in the assessment; and such an assessment may only be given "**conclusive force**" ***at the request of the data subject***. This provisions appears to be wider than the one contained in the Directive, in that it does not specifically refer to decisions based on ***automated*** processing. This suggests that under the Spanish law, individuals are granted the right to challenge **any decision** on them, based on an evaluation of their work, creditworthiness, reliability, conduct or other personal matters.

The UK law gives anyone the right to ***require*** any data controller at any time, in writing, "to ensure that no decision taken by or on behalf of the data controller is based on [fully automatic processing of the kind noted in the description above]". Presumably (although this is not clearly spelled out), in this case (i.e., if such a notice "has effect"), the controller may no longer take decisions of this kind in respect of the person concerned.

Next, the law stipulates that if, "in a case where no [such notice] has effect", a fully automated decision of the above kind is taken, the controller must **notify the individual** "as soon as reasonably practicable" of the fact that the decision in question was taken in this way; and the data subject is then entitled to "***require*** the data controller to **reconsider** the decision or to take a **new decision** otherwise than on that (fully automated) basis. The controller must then, within 21 days, inform the data subject of "***the steps that he intends to take*** to comply with the data subject notice." Presumably (although this is again not clear), the steps must include a **non-automated re-evaluation** of the contested decision.

It should be mentioned that when the data subject is informed of the nature and outcome of the decision, there is no duty on the controller to also inform him of the "logic" used in the

decision (i.e. of the factors relied on in the decision) - even though the data subject does have the right to be given this information on request, as noted above, at 9.1.

However, none of the above applies to what is referred to in the UK law as an "**exempt decision**". Or to put it another way: data subjects do not have a right to require data controllers to refrain from taking fully automated "exempt decisions", and they cannot ask them to reconsider such decisions. There are, in effect, **four kinds of exempt decisions** (and further ones may be prescribed). The first two of these correspond to the first two specified in the Directive, set out above, i.e. decisions taken in contractual (or pre-contractual) context, if *either* the ***request*** of the data subject ***is granted***, *or* if "steps" have been taken to safeguard the legitimate interests of the data subject (for example, by allowing him to make ***representations***). The last two apply the same reasoning to decisions "authorised or required by or under any [law]". In other words (as in Belgium and Sweden) such decisions too are allowed if *either* the ***request*** of the data subject ***is granted***, *or* if the data subject was allowed to make ***representations***. Finally, the Act allows the Secretary of State to **exempt**, by means of an Order, any ***further decisions*** - but no such Order has as yet been issued.

All this does not clarify to what kinds of decisions the above-mentioned rules (that is, the rules which reflect the provision in the Directive) apply. I have myself expressed the view (based on the drafting history of the Directive) that ***Art. 15 of the Directive, taken on its own terms, should only be applied to a very limited range of decisions***. The relevant section from the report in question (section 4.ii(d) from the Report on the Directives, produced for FEDMA\DMA-USA) are attached. The German authors Dammann and Simitis, in their Commentary on the Directive,[79] appear to agree and mention as examples: the selection of candidates for a donated organ, if the criteria for selection go beyond purely objective medical criteria and include social data; or if candidates for jobs, or current employees, are ranked on the basis of psychometric assessments. In other words, the provision is aimed at so-called **expert systems** - and not at the use of computers in more traditional assessments of objective data.[80]

Here, it may be noted first of all that (as shown above) the Member States do not all restrict the relevant rules in this way: the laws in France, Greece, Luxembourg and Spain in particular extend (or appear to extend) the in-principle prohibition to other kinds of decisions. Furthermore, neither in States which (in legal terms) apply the rules broadly, nor in those in which the rules are restrictively phrased, is there as yet much guidance on this matter. In Sweden, this provision has not yet been invoked or applied at all; and the same can be said of other countries, such as the UK. In Austria, the driving test is carried out in part by means of a computer test. The computer evaluates the actions of the person applying for a driver licence and "decides" whether the person is fit to be issued with the licence. However, there is no ruling as to whether the test constitutes the kind of decision caught by the in-principle prohibition or not: as noted above, in that country, the fact that the test is authorised by law means that the matter cannot be tested. In Spain (where, as we have seen, there are two provisions on the matter, one absolute and one conditional), the absolute prohibition would appear to apply, in particular, to evaluations based solely on (psychological) personality traits, while the conditional rules would seem to apply more specifically to evaluations of more measurable aspects of a person's behaviour - but this too has not yet been clarified. Even in

[79] Dammann\Simitis, EG-Datenschutzrichtlinie: Kommentar, Baden-Baden, 1997.
[80] O.c. (previous footnote), margin note 4 to Article 15.

France, where an in-principle prohibition has been in effect for many years, there is little or no guidance from the data protection authorities or the courts.

Overall, this provision is applied **extremely rarely**. Indeed, the UK data protection authority (the Information Commissioner) feels that it is largely **unjustified**:

> "The justification for this Article is unclear. Automated individual decisions will necessarily involve the processing of personal data. Such processing must in any case be "fair". The Article includes a form of partial exemption for decisions taken in the course of entering into or performing a contract. The Commissioner's understanding is that most significant automated decisions fall into this category. The apparent objective of the Article could be achieved much more simply by a requirement that where data subjects are subject to automated decisions that significantly and adversely affect them they should be made aware of this and be given an opportunity to make and have heard representations as to why the decision is wrong. Even this may be overly prescriptive and there may be a case for dispensing with the Article altogether."

ATTACHED: Extract from D Korff, Report on the Directives, FEDMA\DMA-USA, 2002.

- o – O – o -

ATTACHMENT TO SECTION 9.4 (the right not to be subject to a fully automated decision): Extract from D Korff, Report on the Directives, FEDMA\DMA-USA, 2002:

(d) restrictions on the taking of fully automated individual decisions

in-principle prohibition

Article 15(1) of the framework Directive stipulates that Member States must grant every person the right:

> not to be subject to a **decision** which produces legal effects concerning him or significantly affects him and which is **based solely on automated processing** of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Furthermore, under the Directive, data subjects must also be able to obtain:

> knowledge of the **logic** involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1). (Art. 12(a), third indent)

While phrased as a right of data subjects, Art. 15(1) in effect lays down an in-principle prohibition on the taking of fully automated decisions of this kind. It then provides, in para. (2), for two types of exception to this prohibition. As important as these exceptions, however, are the limitations implicit in the definition or description of the type of decisions caught by the prohibition. **It should be stressed that the provision only applies to certain very special kinds of decisions.**

limits of the prohibition: what kinds of decisions are covered

First of all, fully automated decisions are only prohibited if the processing involves an "evaluation of [the data subject's] personal aspects", such as his performance at work, creditworthiness, reliability, conduct etc. – what is referred to in the Explanatory Memorandum to the Amended Proposal as a "**personality profile**". A decision based on simple, objective, verifiable factual data - e.g. the amount of money in an account or the salary someone earns or his or her age - does not involve an evaluation of such "personal aspects": the provision is aimed at decisions involving (or at least getting very close to) a value-judgment:

> "The processing must apply variables which determine a standard profile (considered good or bad) to the data concerning the data subject; this excludes all cases where the system does not define a personality profile: for example, the fact that a person is unable to obtain the sum of money he wants from an automatic cash dispenser because he has exceeded his credit limit would not fall inside this definition." [81]

It may be difficult to draw the exact lines here (for an example on when this could apply to the sending of offers to selected targets, see below) but it is quite clear that the aim of the provision is not to prevent decisions being made by computer if this is on the basis of

[81] Amended Proposal (*supra*, footnote 46), p. 26 (comment on what was then Art. 16 of the draft Directive, which became Art. 15 in the final version).

straight-forward factual data, but rather to provide for safeguards when computers are used to evaluate highly complex, more subjective (or at least less individual-related) factors. The application of statistical data - i.e. of probabilities - to individual cases might be caught by the in-principle prohibition in some cases, and not in others. Thus, the use of age as a factor in health insurance, while of course relating to a probability rather than an individual certainty, would appear to be uncontroversial. However, Member States (and\or, in due course, the Court of Justice) might feel that the use of highly complex geo- or psychodemographical data - or, in the near future, genetic data - should be more closely circumscribed.

A typical example of a profile that does fall within the definition, is the one used in a recently announced "offender assessment system" in the UK. This system, called Oasys, generates a computerised score of "how likely [offenders] are to reoffend and what danger they pose to the public", based on factors including:

> "unemployment, literacy, family circumstances, lifestyle, history, who he or she has mixed with and educational background, as well as on the criminal's attitude to his or her offence."[82]

Second, the decision must be "based **solely** on automated processing". Perhaps the most important aim of the provision is to ensure that important decisions on individuals are not made by computers, without human involvement. It was felt that that would reduce individuals to mere objects in a computer programme, and violate human dignity and fundamental rights. However, this does not preclude the use of automated processing as an *aid* in decision-making, as long as the computer assessment is not conclusive or slavishly followed:

> "The danger of misuse of data processing in decision-making may become a major problem in future: the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities. … Data processing may provide an aid to decision-making, but it cannot be the end of the matter; human judgment must have its place."[83]

The provision is thus again not aimed at preventing the use of computers - and even of sophisticated "personality profiles" created by "expert systems" - in making decisions, but only to ensure that such decisions are not ***solely*** arrived at in this way. The above-mentioned "offender assessment system", for instance, is supposed to only support decisions by the courts:

> "A computer would analyse the results [the above-mentioned factors – DK] and produce a score *to enable an experienced probation officer to predict how likely the person was to reoffend*. … *Oasys would not replace the judgment and gut instincts of probation officers, but would allow their reports, on which the courts based their sentencing, to be less subjective.*"[84]

---

82 "Computer to score chance of criminals reoffending", Guardian, 18 August 2000. Of course, the processing involved in Oasys as such falls outside the scope of the Directive, since it concerns "activities of the State in areas of criminal law" (cf. Art. 3(2)). However, as explained above, at 3.*i*, this does not mean that it would not be affected by the national implementing law. Here, the system is merely mentioned as a good example of "profiling" with significant implications.

83 Amended Proposal (*supra*, footnote 46), p. 26.

84 *Idem*, emphasis added.

If used in this way, Oasys would therefore not be caught by the prohibition.[85] The in-principle prohibition nevertheless has some significant implications, e.g. in the field of employment:

> "It would be contrary to [the principle that a decision may not be solely based on a computer profile], for example, for an employer to reject an application from a job-seeker on the sole basis of his results in a computerized psychological evaluation, or to use such assessment software to produce lists giving marks and classing job applicants in order of preference on the sole basis of a test of personality."[86]

Third, for a decision to be caught by the prohibition, it must produce "**legal effect**" or otherwise "**significantly affect**" the person concerned. Decisions with "legal effect" include, in the public sector, the kind of decisions in which Oasys would be used - decisions on bail or on the length and type of sentence imposed on offenders - as well as decisions on whether or not to grant certain state benefits, and in the private sector, decisions to enter into or terminate a contract (of employment, or concerning the rental of a house, or credit, etc.). Whether a decision not to enter into a contract with someone has legal effect is a moot point, which may be answered differently in different legal systems - but such a decision will, in most cases, be at least considered to have a "significant effect" on the person concerned.

On the other hand, as the Explanatory Memorandum to the Amended Proposal for the Directive expressly clarifies:

> "the simple fact of sending a commercial brochure to a list of persons selected by computer is not a decision adversely affecting them [for the purposes of Art. 15]."[87]

The lines are again not sharply drawn, however, and much will depend on how this provision is implemented in the Member States' laws and applied in practice. Thus, for instance, a mailing by which some selected individuals are offered a substantial benefit (e.g. a particularly attractive credit card or investment opportunity or insurance) denied to others may (if the decision on who to mail meets the other requirements of Art. 15) by some be said to have a "significant" effect (on the people not chosen). However, it should again be stressed that this does not mean that a credit card or investment company cannot send out such offers selectively. Rather, it cannot base the selection solely on a non-factual, value-judgmental kind of personality profile. Selections based on (say) actual income- or spending- or repayment levels, or records of previous investments, or employment status, or house ownership, or age (or a combination of these) would normally not be caught by Art. 15(1) at all. A highly sophisticated scoring system, however, which would take into account geo- and psychodemographic factors might be caught.

---

85 The newspaper report says that "It [Oasys] would **decide** whether a defendant should be freed on bail" (my emphasis), but presumably the system would again only be used to "assist" in this decision. If in time it would transpire that the system was excessively relied on, with the system (rather than the probation officers or the courts) effectively determining the result, then it would be caught by the in-principle prohibition if and to the extent that the national law implementing the Directive would apply in this non-Community area.

86 Amended Proposal (*supra*, footnote 46), p. 26.

87 *Idem*.

10. special exceptions in the laws [Arts. 9 & 13]

introduction

The Directive provides for a number of exceptions or relaxations to its provisions. The study first examined how, in the member States, the rules in the Directive were reconciled with **freedom of expression** and with **freedom of information** (**FOI**, in the sense of a right of access to official documents). Next, it looked at exceptions for **major public interests** (***national security***, ***defence***, the ***investigation and prosecution of offences***, etc.), and for the **protection of the data subjects and others**. In the latter respect it also looked at the rules adopted by the Member States to regulate the use of ***CCTV cameras***.

summary of findings

With regard to **freedom of expression**, the laws in the Member State in this respect are ***wildly divergent***, and range from stipulating the overall primacy of freedom of expression, through wide exemptions for the press, to a system which is tantamount to imposing prior restraint on the publication of certain information by the press. This is clearly an area in which **no serious convergence** can be discerned. A further point is whether Data Protection Authorities are the **appropriate *fora*** for decisions affecting the freedom of the press or freedom of expression generally.

At first glance, it would appear that **FOI** raises principles similar to freedom of expression, in that it is an area in which two fundamental principles must be reconciled. However, in this respect this "reconciliation" causes **less problems**. Specifically, the issue is, in most Member States, much less seen as requiring a choice between competing, hard-to-reconcile interests than as requiring a **general, "balanced" approach** in individual cases - which can be achieved as much under the one kind of law as under the other. Which law "prevails" thus largely become irrelevant. This is important for one Member State in particular, because if this was not the case it would raise serious constitutional issues, reminiscent of earlier conflicts between the German Constitutional Court and the Court of Justice in Luxembourg. owever, in one or two Member States, some problems of conflict between the data protection- and FOI-laws remain.

The laws in all the Member States contain exceptions relating to ***national security***, ***defence***, the ***investigation and prosecution of offences***, etc. (cf. Art. 13(1)(a) – (f) of the Directive) - but there are **quite significant divergencies** between the specific exceptions of this kind in the laws in the Member States examined so far. A number of findings need to be stressed in this regard. First

of all, in spite of these differences, there seems to be a **general acceptance** that ***processing of personal data for police-, public order- and similar purposes can be regulated in accordance with the Directive***, taking into account the possibilities for exceptions provided for in the Directive - with some Member States indeed feeling that those exceptions can be **narrowed further** and\or made subject to **additional formal requirements**. Secondly, the exceptions for these kinds of interests often ***cross-refer*** (and all too often ***defer***) to ***other laws***. Thirdly, as noted below, there is more agreement on the use of CCTV-cameras (also) in the context of public order and safety and the prevention and investigation of crime.

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** and ***the tests applied are quite vague***. Although they generally agree on the need for an exception, or more specific exceptions, to protect data subjects or others, there is therefore again ***no certainty*** that these tests will be applied consistently throughout the Community. On the contrary, they are likely to lead to **further divergencies**.

However, as just noted, with regard to the use of **CCTV-monitoring** there is **greater concensus** on the basic principles and, in some countries at least, **clearer guidance** on the detailed application of those principles. Such guidance tends to focus on the need to ***restrict*** **monitoring** as much as possible, and the need to ***restrict*** **recording** of surveillance data separately, further; and on the importance of ***ensuring openness*** with regard to CCTV use. They stress that with regard to CCTV monitoring of **public places**, this should be done through ***openly displayed*** cameras, and by displaying ***notices***, while in the **workplace** this should involve the providing of **clear rules** to workers, in consultation with **Workers' Councils**.

matters to be further clarified or addressed

The wide differences in the way the **press**, and matters relating to **freedom of expression generally**, are dealt with in the Member States raise **serious problems** in respect of cross-border journalism or cross-border exercise of this right generally. This is a matter that ***needs to be further examined in detail***, with reference to both data protection- and freedom of expression standards, as developed at EC- and wider European level and to the case-law of the European Court of Justice and the European Court of Human Rights in particular. However, it is clear that, in any case, ***Art. 9 of the Directive will need to be rephrased***.

On **freedom of information** and on the use of **CCTV-cameras** it is important to ***confirm and clarify in further detail*** the basic agreement in principle between the Member States, while with regard to exceptions aimed at **protecting the data subject or others *substantial further clarification*** is also essential.

As far as **exceptions for major public interests** such as ***national security*** etc. are concerned, it is important to ***stipulate formally*** that while such exceptions can indeed be based on other laws ("legislative measures") in the Member States, these must be applied in accordance with the Directive, which requires that, in addition, the exceptions are limited to what is "***necessary***" to protect these interests.

- o – O – o -

10. special exceptions in the laws – detailed findings

10.1 exceptions relating to freedom of expression

> "Everyone has the right to respect for his **private and family life**, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society ... [*inter alia*] ... for the protection of the rights and freedoms of others." (Art. 8 ECHR)
>
> "Everyone has the right to the **protection of personal data** concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority." (Art. 8 of the Charter of Fundamental Rights)
>
> "Everyone has the right to **freedom of expression**. This right shall include ***freedom*** to hold opinions and ***to receive and impart information and ideas*** without interference by public authority and regardless of frontiers. ... The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to scuh formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of ... [*inter alia*] ... the protection of the reputation or rights of others ..." (Art. 10 ECHR)
>
> "Everyone has the right to **freedom of expression**. This right shall include ***freedom*** to hold opinions and to ***receive and impart information and ideas*** without interference by public authority and regardless of frontiers. The **freedom and pluralism of the media** shall be respected." (Art. 11 of the Charter of Fundamental Rights)
>
> "Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for ***journalistic purposes*** or the purpose of ***artistic or literary expression*** only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression." (Art. 9 of the Directive)

As will be clear from the references above to a range of fundamental provisions in European law, the relationship between data protection and freedom of expression is complex. Even so, the wording of Art. 9 of the Directive is somewhat odd. It recognises, on the one hand, that the right to privacy and the rules governing freedom of expression need to be "reconciled", and that "exceptions and derogations" are therefore required from a range of provisions in the Directive (or rather, from provisions in the laws implementing the Directive). It is also right to say that such exceptions and derogations should go no further than "necessary" to achieve this, i.e. that the fundamental right to data protection as provided for by the Charter and ensured by Directive (and these laws) should only be limited to the extent "necessary" to protect the competing Charter-protected interest, freedom of expression. However, the Directive unjustifiably stipulates these matters only with regard to "***processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression***": the right to freedom of expression (and the right to [seek,] receive and impart

information) is guaranteed by Art. 10 ECHR and Art. 11 of the Charter to "**everyone**", not just to journalists, artists and writers.

This is explicitly recognised only by Denmark and Sweden. The law in the first country (while also providing for exemptions for collections of published materials and special exceptions for journalists etc., as discussed below) first stipulates quite simply and generally - and rightly:

> "This Law shall not apply where this will be in violation of the freedom of information and expression, [as provided for in] Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms."

The Law in Sweden refers to that country's own constitutional provisions on freedom of expression rather than to the international guarantees, but adopts **the same principled approach** where it stipulates (again, separate from more specific provisions concerning journalism etc.) that:

> "The provisions of this Law shall not be not applied to the extent that they would contravene the provisions concerning the freedom of the press [read: freedom of information] and freedom of expression contained in the Freedom of the Press Law or the Fundamental Law on Freedom of Expression."

Although it will at times be difficult to make these assessments, these provisions are an important recognition of the need to lift or moderate the application of rules in data protection laws which, if fully applied, would unduly hamper the activities, not just of journalists etc., but of ***anyone*** exercising their right to freedom to seek, receive or impart information.

The above-mentioned principled approach has been strongly affirmed in an important judgment of the Swedish Supreme Court, in which that 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:

> CASE EXAMPLE: The case concerned the publication on a website of information and (quite insulting) statements about persons in the banking- and financial world by a Mr Börje Ramsbro. Mr Ramsbro was prosecuted for having transferred personal data abroad in contravention of the Swedish data protection law, which reflects the Directive. The law contains an exemption from the prohibition on such transfers, which however (in accordance with the Directive) only applied to transfers made for "journalistic purposes". Mr Ramsbro claimed that he could rely on this exemption, even though he was not a (professional) journalist. The Supreme Court held:
>
> "[T]he rights according to articles 8 and 10 of the European Convention [on Human Rights] in specific cases may come into conflict with each other. For the purpose of solving such conflicts the European Court of Human Rights applies the principle of proportionality, which means that a balance is truck between the interest of protection of privacy and the interest of freedom of expression. ***It may be presumed that what in the [Swedish data protection law], on the basis of the Directive, has been prescribed about exemption for journalistic purposes is meant as an attempt to express in more general terms such a striking of balance.*** **That the expression journalistic purposes has been used may under such circumstances not be supposed to be meant as priviliging established mass media or persons who are professionally active within such media.**

> **The expression will probably instead have been used in order to emphasise the importance of free distribution of information with regard to issues of importance for the public or for groups or persons and a free debate in societal issues**."[88]

Such considerations are of particular importance to **human rights organisations**, who collect sensitive data for purposes which are not solely "journalistic" in a narrow sense.

However, another case in Sweden, also concerning the publication of information on the Internet, was (so far) less succesful:

> CASE EXAMPLE: The case concerns the creation, by a private individual, of a website on her own computer which contained information about 18 employees of the local Swedish (i.e. Lutheran) Church in a small town in the south of Sweden. The person responsible for the website was preparing children for communion and wanted them to have information about the people in the local church. One of the persons on whom she included information had injured her leg and that was also posted on the website. She did not put up the web pages as part of any employment nor did she receive any remuneration for it. She was then charged with violation of the Swedish data protection law for dissemenating health-related (i.e. "sensitive") information about a person without that person's consent. The case has been referred to the Court of Justice in Luxembourg for a preliminary ruling, where the defendants argue that (to the extent that the case is subject to EC law in general and the Directive in particular, which they deny) the Directive contravenes Art. 10 of the European Convention on Human Rights and thus general principles of Community law. (Bodil Lindqvist –v-. Sweden)

The Luxembourg law contains certain exceptions from the normal rules in that law (further discussed below), for the benefit of processing "carried out ***solely for the purposes of journalism or of artistic or literary expression***", but prefaces this with the *caveat* that those exceptions are "***without prejudice to the rules in the legislation on mass communication media***" and only apply to the extent that they are "***necessary to reconcile the right to private life with the rules governing freedom of expression***". While recognising the broader picture (i.e. the wider need to reconcile the rules relating to these two fundamental rights), the legislator seems to have only considered the possibility that the exceptions might be too wide: that granting them to the media might unduly fail to protect privacy. They do not appear to address the reverse problem, noted above: that not extending these exceptions to others than journalists or the media may unduly restrict freedom of expression of non-journalists. This can perhaps be resolved by interpreting the concept of "journalism" broadly (as in the Swedish Supreme Court case, mentioned above) - but the law not yet having come into force, this is for now unresolved.

The law in Austria contains (in addition to more specific exceptions, noted below) a provision to the effect that the processing of personal data is allowed:

> "to the extent that this is ***necessary to fulfil the information-providing task of*** **media companies, media service providers and their employees** in the exercise of the fundamental right to freedom of expression in accordance with Art. 10 ECHR."

---

[88] Judgment B 239-00 of the Swedish Supreme Court *on the European Parliament and the Council 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*, Swedish Helsinki Committee for Human Rights, Stockholm, 2001, p. 9.

While also referring to Article 10 of the Convention, this provision too is ***much more limited*** than the general ones in the Danish and Swedish laws, both in only applying to **media entities** and in being limited to **processing which is "necessary" to inform the public**. Neither of these limitations is of course contained in Art. 10 ECHR itself. On the contrary, the right to freedom of expression (while it can be limited to protect other interests) extends to the right to disseminate quite "unnecessary" information, by the media or anyone else. Moreover, under the Convention, the limitations on the exercise of this right must be "necessary", not the exercise itself.

In addition to the above (and to a more limited exception for journalists etc., discussed below), the law in Denmark also basically does not apply to processing of personal data covered by the Law on information data bases operated by the mass media, or to information data bases which exclusively include ***already published periodicals or sound and vision programmes***, or ***already published texts, images and sound programmes***, which are regulated by the Law on the responsibility of the mass media, provided the texts or recordings are in their ***original form***. However, certain rules on data security and liabilities do apply.

The law in Finland also **exempts** from its provision altogether any "***personal data files containing***, ***solely and in unaltered form***, **data that have been published by the media**". This exemption primarily applies to the storing of ***newspaper cuttings*** but must be assumed to also extend to the storing of (unaltered) media reports in ***digital form*** (e.g., as downloaded from the Internet) and indeed to the keeping of "structured" records of ***audio-, photographic- or video-images***, if they are made "easily" accessible with reference to the data subjects by means of an index. However, the exemption is lost if any additional data are added, or if the records are in any way modified. Otherwise, the law in Finland provides for an exception only with regard to journalistic (*et al.*) processing, as noted below.

The Spanish law does not refer to freedom of expression at all, not even with regard to these more limited areas. 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. This is said to be because in Spain the data protection law is seen as a specific measure of regulation of the constitutionally-protected right to freedom of expression: although this is not expressly stipulated, the law will under the Constitution only be applied to processing in the context of the exercise of that right to the extent that it does not unduly interfere with the freedom of "everyone" to seek, receive and impart information, and the freedom of the press in particular. However, the same can be said about most of the laws in the Member State which give supra-statutory protection to freedom of expression, and the absence of more specific exemptions or exceptions from the Spanish law therefore remains problematic, as the following case may show:

> CASE EXAMPLE: The Spanish data protection authority imposed a sanction on a private association which compiled annual reports regarding torture and which created a file (published in Internet) containing names, places and data on the state of the procedures against officials alleged to have been involved in such abuse, indicating if the person was convicted, acquitted or if the procedure had not yet reached the end.
>
> The authority held that the information published on the Internet constituted a structured set of data, which fulfilled the legal definition of "filing system", and was therefore

> subject to the Spanish datra protection law. The data protection authority also held that publication of the file on the Internet was to be considered as communication of data. The association could not prove that all the data was obtained from data subjects or public accessible sources. Furthermore, according to the Spanish data protection law, personal data on criminal or administrative offences may only be included in files of the competent public administrations and under the circumstances laid down in the respective regulations (see above, at 7.5).
>
> Although the association sought to rely on the right to freedom of expression, it was penalised for keeping a file containing personal data on criminal or administrative offences. According to the data protection authority, the right to freedom of expression could be exercised through publishing the annual report, which was beyond its competence: the annual report is not to be considered as a file.

The laws in the other Member States provide for exemptions from or exceptions to their data protection laws for the **press**, **journalists** or "**journalistic, artistic or literary purposes**" only. The exceptions in these and the other countries already mentioned ***vary considerably***.

Under the laws in Finland and Sweden, **processing of personal data "for purposes of journalism or artistic or literary expression"** is subject to **selected provisions** in the laws concerned only. These mainly concern the duty to ensure adequate ***security*** and ***supervision*** over adherence to that specific duty, but also include the "***applicable law***" provisions in these laws, discussed below, at 4.1. This means that (wittingly or unwittingly) these exceptions have extraterritorial effect in some circumstances, but do not apply to processing in Finland or Sweden by non-Finnish\Swedish journalists, artists or writers in other circumstances. The law in Denmark also (in addition to the general exemption mentioned above) expressly limits the application of the law to processing for these purposes to the provisions on ***data security and confidentiality*** and ***civil liability*** for breaches of these provisions, but is less clear as to the question of "applicable law".[89]

In France, the tension between freedom of the press and data protection (but not, suprisingly, the wider tension between data protection and the exercise of freedom of expression by others) was given detailed attention some years ago, in 1995. This led to the **writing and audiovisual media** being given a number of ***exemptions*** from some of the requirements of the current law, provided they complied with the separate constraints in the **press law** and **professional rules**, and provided each media enterprise appointed a **liaison person** with the data protection authority (i.e., in effect, an ***in-house data protection official***, of the kind further discussed below, at 12). The proposed new (amended) law confirms and extends these exemptions, and adds exemptions with regard to processing for the sole purposes of **literary or artistic expression**. The proposed law will **exempt** processing for those purposes, or carried out solely "in the exercise of ***professional*** **journalistic activities**", from the restrictions in the law on the processing of ***sensitive data*** and data on ***criminal convictions***

[89] The Danish law contains a further (and perhaps somewhat redundant) exemption for "manual files of cuttings from published, printed articles which are exclusively processed for journalistic purposes". The limitation of this exemption to "journalistic purposes" would appear to be unwarranted, in that it would normally also be an unjustified interference with the right to freedom of expression and information to prevent ordinary people (not just journalists) from keeping newspaper- and magazine cuttings. In this, they can rely on the general clause, mentioned earlier. This exception is also subject to the exception concerning security and damages for breach of security - although I would have thought that the security requirements for a collection of newspaper cuttings cannot be very high, nor could much damage result from the "leaking" of such already-published information.

etc., from ***notification*** and from ***the duty to inform data subjects*** and grant them their ***rights of access and correction***, and from the restrictions on ***transborder data flows***. However, as before, **journalists** (and the enterprises they work for) only benefit from these exemptions provided that they act in accordance with their ***professional rules of conduct*** and provided the enterprises concerned appoint a **liaison person**. The law also expressly emphasises that the exemptions (for journalists as well as those for artists and *literati*) are **without prejudice** to the (strict) legal rules in France relating to the exercise of freedom of expression, i.e. the ***civil- and criminal-legal rules of defamation*** (which in France, as in most other Continental-European countries, apply not just to factually wrong data affecting a person's standing, but also to the dissemination of such data without legitimate cause ["**public interest**"]), the **press laws** and the specific legal rules on the ***right to reply***, etc. The effect of the limitation of the exemptions to the media can be illustrated by the following case:

> CASE EXAMPLE: certain persons in France who were concerned about the alleged influence of **freemasons**, published a list of members of that society on the ***Internet***. The French data protection authority established that the data had not been made public by the data subjects, and that ***the persons who published the list did not benefit from the exemption extended to the press***. It speedily intervened and obtained the closure of the site (and indeed of a "mirror-site" in Belgium).

The point to be made is that, if the publication had been affected by the press, the French data protection authority could not have intervened (although the individuals whose membership of the society had been revealed moght have had a remedy under the press law and\or the laws on defamation).

The law in Germany as such also subjects the **media** only to the provision contained within it on ***data security and –confidentiality***, and on ***civil liability*** (and stipulates that, to the extent that such matters are regulated by State law, the *Länder* must follow this same approach) - but the Law also notes that such processing is regulated further in (fairly strict) **codes of conduct**, which provide for (limited) access to data held by the press and, in particular, for a right to correction of erroneous information. In any case, the "***media privilige***" (as it is called in Germany) is not meant in any way to exempt the media from data protection requirements, but merely to recognise that the balance between the interests of data subjects and controllers must be struck differently in that context.

The Law in the Netherlands **exempts** processing for "**exclusively journalistic, artistic or literary purposes**" from ***a more limited range of provisions***.[90] Such processing is not subject to the ***duty to inform data subjects***, to the exercise of ***data subject rights***, or to ***notification*** and ***prior checks***. The Law however does not exempt such processing from the ***data protection principles and –criteria*** (except for a qualified exemption to the in-principle prohibition on the processing of "sensitive data"), because it was felt that these were phrased in sufficiently flexible terms anyway. The Portugese law takes a similar approach, by exempting processing carried out solely for ***journalistic purposes*** or the purpose of ***literary or artistic expression*** from the duty to inform data subjects, and by granting only **indirect subject access** in such case, in that such access will only be provided through the data protection authority (in the same way as is done with regard to national security or police files). The Luxembourg law contains limited (and, as noted above, qualified) exceptions for

[90] Such processing (or rather, processing by "the press, radio or television", which is not exactly the same thing) was fully exempt from the previous Dutch data protection law.

the benefit of "journalistic processing" concerning the processing of **sensitive data** (but only to the extent that they relate to matters "***manifestly made public by the data subject***" or ***closely related to the public character of the data subject or of the matters in which [that person] is involved***); concerning **transfers of data** to countries without "adequate" protection; concerning the duties to **inform** the data subject (if this would impede the collecting of data, or threaten a planned publication, or might expose sources); and concerning the **right of access** (but the law adds the data protection authority must be granted access, on behalf of the data subject, to unpublished data held for journalistic purpose). **Notification** of processing for journalistic, artistic or literary purposes is moreover limited to information about the name and address of the controller (and his representative, if any).

The Belgian law contains certain much more specific, and thus limited, exemptions with regard to the **processing of data for "journalistic, artistic or literary purposes**". These partly depend on whether the data were ***made public by the data subject*** or relate to ***a person's public position***; the Law also (unlike the Directive) clarifies matters that should be taken into account in determining whether the exemptions can be relied upon, such as the ***protection of sources***, or ***whether the normal rules would hamper the collection of information***.

The Austrian law contains (next to the more general exception concerning processing as part of the media's "information-providing task", linked to Art. 10 ECHR, mentioned above) a further exception according to which **media companies, media service providers and their employees** are, in their "***publishing activities***" only subject to the provisions on ***data security*** (also if they use a processor) and to the ***data protection principles*** (e.g., re "fair" collecting and processing, purpose-limitation and data retention). However, it adds to this that "otherwise, the provisions in the Media Law apply", including in particular the provisions in that law about the protection of the privacy and other "personality" rights of individuals.

The UK law also contains a **highly qualified exemption** for processing for ***journalistic, artistic and literary purposes***. Subject to certain ***complex substantive and procedural conditions***, personal data which are processed for any of these purposes "**solely with a view to publication** of any journalistic, literary or artistic material" and which 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***. The conditions are difficult to fully understand (the Information Commissioner herself called them "almost impenatrable") - but were designed to ensure that in practice the emphasis would remain on the **self-regulatory control** of the press under the **press code of practice**.[91] However, the recent judgment in Naomi Campbell –v- the Mirror Group of Newspapers (QBD, Morland J., 27 March 2002) - which concerned the publication of photographs of the model (taken without her consent and unfairly and unlawfully) which showed that she had attended "Narcotics Anonymous" meetings - established that ***the relevant provision dealt only with pre-publication processing***, and was aimed at ***preventing*** a disproportionate restraint on freedom of expression by measures such as the granting of ***injunctions to stop publications***. The proposed new (amended) Irish law contains an almost identical exemption, and may therefore

[91] A separate exception relating to the **disclosure** of "***sensitive data***" for journalistic, artistic or literary purposes has been included in a special Order concerning the processing of such data. However, as noted above, at 7.4, this further exception appears to be aimed primarily at persons who provide data on unlawful or otherwise wrongful acts to journalists or writers (i.e. at so-called "whistleblowers"), rather than at the journalists or writers themselves (who benefit from the wider exemption discussed in the text).

have to be read in the same way. Indeed, given that freedom of expression is expressly protected as a fundamental right in the Irish Constitution, one might assume that data protection should, in that legal system, be more generally balanced against freedom of speech and publication. However, in certain cases this matter was given no special attention:

> CASE EXAMPLE: In Ireland, the data protection authority dealt with a company which photographed athletic events and put the **pictures on the web**, for sale to competitors and others, without having asked the competitors for their permission. After consultations, the company agreed to change its practice and only release its photos with the ***agreement*** of the persons photographed. The authority does not appear to have considered - and the company does not appear to have raised - the question of whether the publication of the photos on the web constituted a (constitutionally-protected) exercise of freedom of expression.

The law in Italy, too, contains only a **limited exception** relating to "***processing of sensitive data in the exercise of the journalistic profession***". This grants certain exemptions from the need to obtain either the consent of the data subject or authorisation from the Data Protection Authority for the processing of "***sensitive data***". However, the law stresses that journalists must continue to abide by the general legal rules relating to journalism and freedom of the press, including the rule that **data on private matters may only be reported if their is a "substantial public interest" in doing so**, unless the data subject him- or herself made the data public or if their publication is justified in view of the public conduct of the data subject. As in the UK, the law strongly encourages the drafting of special **press codes of practice** to clarify the rules in this regard. However, unlike the UK, in Italy the Authority takes a very active role in this drafting, and can impose changes to a draft code. If a (thus possibly amended) code is approved (in the sense of being published in the Official Journal), the Authority can ***prohibit*** processing in violation of the code.

Finally, in Greece, the Law only exempts the **press** from the duty to ***inform*** data subjects, and even then only if the data subjects are "***public figures***". The Law also 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. These rules constitute ***severe restrictions*** on the exercise of press freedom; the requirement of a prior **permit** for the processing (and thus effectively for the publication) of sensitive information on "***public figures***" even amounts to what is known as "**prior restraint**" on the press - something which is regarded as unconstitutional in many other countries and which is also likely to breach the European Convention on Human Rights.

The limitation of the above-mentioned exceptions to "the **media**", "the **press**", "**journalists**" etc. begs the question of what these terms cover. Apart from Sweden (where, as we have seen, the Supreme Court gave a very wide interpretation of the word "***journalistic***"), most countries do not define these terms, let alone what is to be regarded as "***artistic***" or "***literary***". At a time when disseminating information to the public can be done by anyone or any group through simple websites, without the need for elaborate media infrastructure, the scope - indeed the validity - of such exceptions becomes extremely questionable. Also, while it would appear that such exceptions do not benefit publishers of purely **factual data** (such as ***directories***), it is again becoming increasingly difficult to draw the line: in on-line publications in particular, factual and more "journalistic" information is often combined or linked, e.g. if a link is provided on a directory webpage to another page where the user can find an interview with the listed person.

For the purpose of this analysis, the main point to be made is that the laws in the Member State in this respect are clearly **wildly divergent**, and range from stipulating the overall primacy of freedom of expression, through wide exemptions for the press, to a system which is tantamount to imposing prior restraint on the publication of certain information by the press. Also, some defer expressly to press laws or (self-regulatory or quasi-imposed) codes of conduct and associated regulatory mechanism, while others set out the relevant rules in the data protection law itself. This is clearly an area in which **no serious convergence** can be discerned.

A further point which may be noted is the problematic involvement of the data protection authorities in press matters in some countries. In Greece, the data protection authority refused permission for the recording and broadcasting of the "***Big Brother***" television show (in which the public can follow the - usually rather boring - activities of a number of "inmates" of a house through a multitude of video-cameras). Leaving aside whether the decision was in substance in accordance with freedom of expression, the question arises whether data protection authorities are the appropriate *fora* for such decisions.

10.2 exceptions relating to freedom of information

> "Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive;" (72nd Preamble)
>
> "Member States [of the Council of Europe] should guarantee the right of everyone to have access, on request, to official documents held by public authorities. This principle should apply without discrimination on any ground, including that of national origin.
>
> Member states may limit the right of access to official documents. Limitations should be set down precisely in law, be necessary in a democratic society and be proportionate to the aim of protecting ... [*inter alia*] ... privacy and other legitimate private interests" (Council of Europe Committee of Ministers Recommendation R(2002)2 of 21 February 2002, Principles III and IV.1.iv)
>
> "Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to European Parliament, Council and Commission documents." (Art. 42 of the Charter of Fundamental Rights)

The **right of access to official documents**, usually referred to as "***freedom of information***" or ***FOI*** is increasingly recognised as a fundamental right in developed democracies.[92] It has been a fundamental constitutional principle in Sweden since the 18th Century and is also provided for in the Constitutions of Belgium, Finland, the Netherlands and Spain. It is supported by specific legislation in all the EU Member States, with the notable ***exception*** of Germany and Luxembourg (where, however, proposals are under consideration).[93]

---

92 See: Freedom of Information as an Internationally Protected Human Right, by Toby Mendel, Head of Law Programme, ARTICLE 19, London.

93 For details and links to the various laws (worldwide) see: http://www.privacyinternational.org/issues/foia/index.html.

FOI is also given increased recognition in international instruments. As noted above, it has been expressly included in the list of rights in the EU Charter of Fundamental Rights (even if, in that instrument, the right is limited to documents held by the organs of the Union); and its importance was reaffirmed in the Council of Europe Recommendation quoted above, which was adopted as recently as February of this year.

As is clear from the 72nd (and last) Preamble to the Directive, these principles may be "taken into account" by the Member States in their implementation of the Directive. However, this rather vague acknowledgment of the competing principle of freedom of information does little to clarify how the balance must be struck.

Indeed, at first glance, it would appear that FOI raises principles similar to freedom of expression, in that it is an area in which two fundamental principles must be reconciled. However, it appears that in this respect, in most Member States, this "reconciliation" causes **less problems**. Specifically, the issue is, in most Member States, much less seen as requiring a choice between competing, hard-to-reconcile interests than as requiring a general, "balanced" approach in individual cases - which can be achieved as much under the one kind of law as under the other. Which law "prevails" thus largely become irrelevant.

Thus, in Denmark, the law expressly stipulates that the rules in the FOI Law apply with regard to the providing of access to personal data, contained in an official document. However, these rules allow for denial of access if their disclosure would infringe another person's privacy. They are therefore, in principle, in accordance with the data protection law, and with the Directive. In Finland, the situation is on paper the reverse, in that the data protection law stipulates that the right of access to public documents is to be applied in accordance with the data protection law when the access request concerns personal information. However, the effect is the same as in Denmark: the rules applied in either context require a "balancing" of interest, with due weight being given both to the rights of individuals to gain access to information on them, held by public authorities, and to their right not to have such data disclosed to others without good cause under FOI legislation.

The same applies in countries in which this has not been formally clarified in the law. In Austria and Italy, the data protection laws clearly set out the ***general constitutional approach*** to the processing of personal data and the right to privacy (or "intimacy"), including both the providing of access to data subjects and the disclosure of information to others; and this approach also applies to FOI access requests. The same is true in Belgium, Greece and Spain and also expressly confirmed in the Explanatory Memorandum to the Dutch data protection law. The need to apply a consistent approach under either law is also recognised in the UK, in which this is emphasised by the fact that the Data Protection Commissioner is also given the task of supervising the application of the Freedom of Information Act (and was renamed the Information Commissioner in the process).

In all these countries, data protection and freedom of information are seen as two sides of the same coin, with a similar (indeed, identical) "weighing of interests" being required under either law.

However, in Ireland, data protection and freedom of information are still dealt with separately, in two distinct laws, without clarification about their relative status, and which are administered by two different Commissioners). In some respects, the two laws apply

different standards, e.g. as concerns access to documents containing information on other persons, as noted above, at 9.1. The relationship between the laws, and the question of the relative responsibilities of these Commissioners, is therefore described as "delicate" and as yet unresolved. The proposed new (amended) data protection law, too, does not resolve this.

In France, there has been similar confusion under the current (pre-implementation) law, with the freedom of information law generally allowing for the release of certain lists of names (e.g., of the names and functions of officials, or of persons with a hunting licence), which under the data protection law should not be released. In spite of the fact that the French data protection authority has opposed such releases, the highest administrative court (the *Conseil d'Etat*) has ruled in favour of the release of the documents. Although the data protection authority has warned that this could contravene the Directive (insofar as the data concerned are within the scope of that instrument), the proposed new (amended) law confirms the current position, by stipulating that persons who may obtain information (including third-party personal information) contained in public-sector documents under the freedom of information law "shall not be regarded as "***unauthorised third parties***".

The case of Sweden deserves special attention because of the historically high regard for the principle of access to official documents in that country, already noted. In the course of the lengthy process of the adoption of the Directive, Sweden was particularly concerned that the rules in the Directive might clash with its constitutional rules on freedom of information.[94] The adoption of the 72nd Preamble (referred to above) was one result of this concern.

At the domestic level, this matter was given considerable attention. A report by a Government-appointed Committee concluded, in 1993, that there was a **conflict** between the Swedish constitutional rules and the Directive (as then drafted) - but after an extensive consultation exercise and the adoption of the Common Position the Government concluded that there was no conflict. More specifically, a new committee was asked to look at the question again after the adoption of the Common Position on the Directive - and this committee concluded that the Directive is **compatible** with the Swedish constitutional principle of public access to official documents (and *vica versa*). The 1998 data protection law, adopted in order to implement the Directive, is based on this conclusion.

I believe that the latter committee, and the Government, are right. Specifically, the Freedom of the Press\FOI Law is subject to a large number (some 160) exceptions (contained in the Secrecy Law), specifically aimed at reconciling the constitutional openness-principle with other interests. The rules protect economic as well as other personal matters. Of special interest is the general rule in Chapter 7, section 16 of the Secrecy Law which stipulates that access may be denied to official documents containing personal data if there is a reason to believe that the data might be processed in violation of the Personal Data Act. In fact, each of the many provisions in the Secrecy Act is the result of a balance of interest, and according to some provisions a further balance of interest assessment is required in each case. Another example of this striking of a balance can be found in Chapter 2 Article 3(2) of the Freedom of the Press\FOI Law, which refers to provisions in the many special laws and regulations regulating personal data files held by public authorities, and which limit the search criteria

[94] In Sweden, the rules on access of official documents are enshrined, not in a separate law (often referred to as a "Freedom of Information" or FOI law), but in the Freedom of the Press Law. To avoid confusion for those unfamiliar with the Swedish legal system, I will therefore refer to the law concerned as the Freedom of the Press\FOI Law.

that may be used. There might, for example, be a prohibition in a special law or regulation on the use of sensitive personal data, as defined in the Directive, as search criteria, thereby making it impossible to compile a list of persons with personal characteristics defined as sensitive.

The Swedish approach is therefore in fact no different from what I found in the other Member States – it is just that the Swedes have, over the years, elaborated more on the subject, and are (rightly) particularly concerned to preserve their tradition of openness (which indeed they are endeavouring, with some success, to extend to the EU itself). In sum, the provision in the Swedish data protection law that its provisions do not apply "*to the extent that they would limit an authority's obligation under Chapter 2 of the Freedom of the Press Law to provide personal data*"[95] is **not contrary to the Directive**, because the rules in the latter law ensure that the balance required under the Directive is adhered to also in that respect.

10.3 exceptions relating to major public interests

> "This Directive shall not apply to the processing of personal data ... in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law"
>
> (Art. 3(2), first indent, of the Directive)
>
> "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
>
> (a) national security;
>
> (b) defence;
>
> (c) public security;
>
> (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
>
> (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
>
> (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); ..."
>
> (Art. 13(1)(a) – (f) of the Directive)

As noted above, at 2.3, the Member States have generally not availed themselves of the possibility to limit the scope of the national laws adopted in order to implement the Directive to matters within the scope of Community law.

---

[95] The Law adds to this a further provision under which "blocking" of data shall not prevent the release of the "blocked" data if the release is required under the Freedom of the Press\FOI Law.

They have also made ***very 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, quoted above. The law in Denmark fully exempts processing by the **police intelligence branch** and the **security services** from its scope; the Irish law fully exempts "personal data that in the opinion of the Minister [for Justice] or the Minister of Defence are, or at any time were, kept for the purpose of safeguarding the **security of the State**" (and this exemption is to be retained in the proposed new (amended) law); the UK law also contains an almost complete and in practice unchallengable exemption (from the data protection principles, from the exercise of data subject rights, from notification and from enforcement) for the benefit of **national security**; and the Spanish law does not apply to files relating to **terrorism** and to **serious organised crime**. But these are exceptions.

Some countries subject some or most processing in the areas listed in Art. 3(2), first indent, of the Directive to **separate laws**, but this does not necessarily mean that they are not subject to a regime which is (or which is at least supposed to be) compatible with the principles of the Directive. Thus, the special laws on processing by the **police** and the **security services** in the Netherlands, which are in any case already based on comparable principles, are to be brought into line with the Directive (subject to exceptions, but which are also to be in line with the Directive) in the near future. In Italy too, processing in connection with **defence**, **state security**, **police matters** etc. is subject to special laws or rules which must conform to the basis principles in the data protection law. The Luxembourg law stipulates that processing by the police and custom authorities in relation to the **prevention, investigation and prosecution of criminal offences**, processing relating to **state security**, **defence** and **public security**, as well as processing in connection with **Europol** and **Interpol** shall be regulated by Grand-Ducal decree - but the law not having yet come into force, no such decree has been issued either.

In Germany, processing by the **police** and the **security services** is subject to special rules in special laws which are supposed to conform to the constitutional data protection principles (although in some rare cases this can take a long time). In Portugal, the data protection law in principle applies to processing of data for purposes of public safety, national defence and State security "without prejudice to special rules in intruments of international law to which Portugal is bound and specific laws pertinent to the respective sectors" - but the constitutional framework discussed above, at 3.4, there too ensures that even such special rules and laws must be applied in accordance with relevant fundamental principles. As we have seen, in Sweden, rules in other laws and Government regulations in principle override the rules on the data protection law - but an extensive review has taken place to ensure that those other laws and regulations all comply with the Directive.

This is not to say that processing for the kinds of purposes mentioned above and which is (in principle) subject to the national laws implementing the Directive does not benefit from **extensive exceptions and exemptions** within those laws. Indeed, as is clear from Art. 13(1), paras. (a) – (f), also quoted above, the Directive expressly allows for exemptions and restrictions from the data protection principles (Art. 6(1)), the informing-requirements imposed on controllers under Arts. 10 and 11(1), the right of access, rectification or erasure (Art. 12), and the duty to publicise details of processing operations (Art. 21) with regard to such processing. However, the Directive does impose two conditions in this respect: such exemptions or restrictions must be provided for in "**legislative measures**" and they must be

"**necessary**" to safeguard the public interest in question.[96] In terms of the Directive, compliance with these requirements should furthermore be subject to **monitoring** by a "supervisory authority" fulfilling the requirements of Art. 28 of the Directive, as discussed below, at 16 (although it would be compatible with the Directive for States to establish separate authorities for processing in such special areas, as has indeed been done in some of them).

Limitations on the above kinds of matters for the above kinds of purposes are indeed set out in the above way in the laws of Austria, Belgium and Denmark: they all (in somewhat different terms) ensure that processing for police matters, public security, etc. is limited to what is "***necessary***" (or indeed, as the law in Denmark puts it, "***vital***") for those purposes, and that exceptions to a controller's informing-duties and the exercise of data subject rights are also limited to what is "***necessary***" in those regards. In addition, the laws in these countries stress that the application of such exceptions remains subject to **supervision** by the national Data Protection Authority.

The law in Spain used to allow for exceptions from the rights and duties mentioned above when compliance with them would "impede" relevant public interests, or would "pose risks" to them, or indeed if on balance such rights and duties should "give way" to the public interests concerned - but the Constitutional Court (in the ruling discussed at 3.4) held that most of these wide exemptions - and in particular those relating to (unspecified) **monitoring and verification functions**, and to the prosecuting of **administrative** (i.e. minor, non-criminal) **offences** - were ***unconstitutional*** and therefore ***invalid***.[97]

Some Member States indeed impose ***more limited exceptions*** and ***more stringent control*** than envisaged by (permitted under) Art. 13(1). Thus, the law in the Netherlands does not provide for exceptions to the ***data protection principles***, because it is felt that those principles are couched in sufficiently flexible terms anyway. Apart from the full exemption concerning State security, noted above, the law in Ireland, too, only contains exemptions and exceptions as concerns ***disclosures*** and ***subject access*** (as noted below), but no such exceptions with regard to the data protection principles (and this is not to be changed in the proposed new (amended) law).

Neither the current nor the proposed new law in France contain general exemption clauses for the benefit of the public interests listed in Art. 13(a) – (f) of the Directive. Rather, the law stipulates that the **right of access** is to be granted only ***indirectly***, through the medium of the data protection authority. The authority has also closely examined **disclosures** of data (in particular within the public sector), as the following case may illustrate:

> CASE EXAMPLE: The French data protection authority acted against a "***fishing operation***" in which an investigative authority, specialising in detecting violations of employment law, tried to "***match***" data on different public-sector lists, including the list of beneficiaries of **employee health insurance**, to identify possible ***illegal immigrants***

---

96 Note that this reflects the approach to limitations on fundamental rights adopted in the European Convention on Human Rights, which also generally allows for restrictions on the protected rights only when these are "**in accordance with law**" or "**prescribed by law**" and "**necessary in a democratic society**". Cf. the texts of Arts. 8 and 10 ECHR, quoted under the heading to section 10.1, above.

97 The Court upheld exemptions aimed ay protection national defence, public safety or the prosecution of criminal offences - but these are of course "in any case" outside the scope of the Directive.

> (apparently, partly by reference to ***names*** which could reveal national or ethnic origin). It held that such generalised matching of databases, although carried out for a legitimate and important public interest, violated the data protection law.

In Finland, exceptions from data subject rights are limited to those required to safeguard **national security**, **defence**, **public order or -security**, the **prevention or investigation of crime**, or if the personal data in the file are used in the carrying out of **monitoring or inspection functions** and not providing access to the information is **indispensable in order to safeguard an important economic interest or financing position of Finland or the European Union**. The last-mentioned exception is much more limited than what is envisaged in paras. (f) and (g) of Art. 13(1) of the Directive, which between them allow for exceptions for *any* monitoring function related to the exercise of official authority, and for *anything* to do with those economic and financial interests. To this the law 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 contains provisions under which the **informing-requirement**s and the **rights of access, rectification and erasure** do not apply to "***processing which is necessary***" for the kinds of matters listed in Art. 13 of the Directive: **State security**, **defence**, **public security**, activities of the State in the field of **criminal law**, **important economic or financial interests of the State or the EU**, or **to protect the data subject or the rights and freedoms of others** - which is not the same as allowing exceptions to these requirements only to the extent that those exceptions are required in every individual case. However, the Luxembourg law also stipulates that if controllers refuse or defer access on these grounds, they must set out the **reasons** for this refusal or delay - and adds that ***the data protection authority must be informed of these reasons***. This should ensure that the exceptions are restrictively applied, in accordance with the Directive (but there is of course as yet no practice under the law). The law in Greece goes even further, in that it 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.

Apart from the very wide exemption with regard to processing for the purpose of safeguarding national security, mentioned above, the law in the UK includes a series of more limited exemptions for personal data processed in relation to **crime and taxation** matters, **health, education and social work**, and **regulatory activity** related to ***prevention against fraud, dishonesty or malpractice***, the activities of ***charities***, ***health, safety and welfare of persons at work***, ***maladministration (etc.) by public bodies***, ***fair trading*** etc. Most of these exceptions are limited to what the UK law calls the "subject information provisions", i.e. the informing-requirements (discussed above, at 8) and the data subject access requirements (discussed above, at 9.1), but the "crime and taxation"-exception extends to the "fair processing"-principle. The main point to be made about these exceptions however is that they all 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. This is confirmed by the

UK dat protection authority, the Information Commissioner, who has stressed that these exceptions are restrictively applied:

> "The Commissioner takes the view that, for any of these three exemptions to apply, there would have to be a **substantial chance** rather than a mere risk that in a ***particular case*** the purposes [crime prevention and –detection and taxation] would be ***noticeably damaged***. The data controller needs to make a judgment as to whether or not prejudice is likely in relation to the circumstances of each case."

As mentioned earlier, apart from the full exemption with regard to data kept for the purpose of State security, already noted, the current Irish law also contains some further exemptions relating to **disclosures** of data for the purpose of safeguarding the ***security of the State***; to protect the ***international relations of the State***; or for the purpose of ***preventing, detecting or investigating crime***; or. The first rests simply on the basis of the opinion of a senior police or army officer; the second must be "required" to protect the relations concerned; while the third one (concerning crime) only applies if the application of the normal restrictions on disclosures "would be ***likely to prejudice***" the crime-tackling measures in question. The first exemption is therefore effectively beyond the scope of judicial review or supervision by the data protection authority; the second is subject to limited review; while the third can - as in the UK - be made subject to quite strict supervision by the national data protection authority and the courts. The Irish law also contains a series of **exceptions to the right of subject access** with regard to personal data kept for the purposes of preventing, investigating or prosecuting criminal offences, assessing or collecting taxes, maintaining security in prisons, protecting people against fraud or malpractice, etc. – but these too only apply to the extent that allowing access to the data "would be ***likely to prejudice***" the matters concerned, which again equates to the "***necessity***" test in the Directive. On the other hand, the law also contains a few provisions which exempt data from subject access without applying such a test: this concerns data kept "for the purpose of discharging a function conferred by or under any enactment and consisting of information obtained for such a purpose from a person who had it in his possession for any of [the above-mentioned purposes (action against crime or in relation to taxation, et.c)]"; and data "in respect of which [subject access] would be ***contrary to the interests of protecting the international relations of the State***". These provisions are to be retained unchanged in the proposed new (amended) data protection law.

In practice, the Irish data protection authority has given considerable attention to the **disclosing of information by public and private bodies to the police**, and extensive discussions are taking place on these matters between the Commissioner's office, the *Gardai* and the Ministry for Justice. In addition, the Commissioner is in the process of taking a decision on **data exchanges between Government departments** in cases corresponding to those covered by Art. 13(1)(f) (monitoring, inspection and regulatory functions).

There are in these respects therefore again **quite significant divergencies** between the laws in the Member States examined so far. However, it is important to note that there seems to be a general acceptance that processing of personal data for police-, public order- and similar purposes can be regulated in accordance with the Directive, taking into account the possibilities for exceptions provided for in the Directive, such as in particular those set out in Art. 13(1)(a) – (f)) - with some Member States indeed feeling that those exceptions can be narrowed further and\or made subject to additional formal requirements.

10.4 exceptions relating to the protection of data subjects or others (including CCTV monitoring)

> "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard ... the protection of the data subject or of the rights and freedoms of others." (Art. 13(1)(g) of the Directive)

Not all the Member States feel the need to adopt a general exception clause on the lines suggested by Art. 13(1)(g). **No such general provision** is included in the law in Belgium, where the legislator felt that the ordinary rules and exceptions concerning specific matters were flexible enough anyway. There is also no general exception of this kind in the French (current and proposed new), Luxembourg and Portugese laws. As explained above, at 3.4, the Swedish general data protection law leaves these matters to be determined in other laws and therefore also itself does not contain such ageneral provision.

The other laws all contain **general exception clauses** or **more specific clauses** allowing restrictions on the matters mentioned, and in particular on the exercise of data subject rights, in order to protect the data subject or others (including the controller) - but they apply ***different tests*** in this regard.

Thus, as already noted in the previous section, the Luxembourg law contains provisions under which the informing-requirements and the rights of access, rectification and erasure do not apply to "***processing which is necessary*** ... [*inter alia*] ... ***to protect the data subject or the rights and freedoms of others***". Again, the added requirement that the **reasons** for reliance on at least the latter of these exceptions must be ***noted and passed on to the data protection authority*** should ensure that in practice these provisions will be restrictively applied.

The law in Finland allows controllers to deny access to data if "providing access to the data would cause **serious danger** to the ***health or treatment of the data subject*** or to the ***rights of someone else***" - which is stricter than the "necessity" test laid down in Art. 13(1)(g). The law in the Netherlands uses the same wording as the Directive - but the Explanatory Memorandum to the law stresses that the "necessity" test should be applied ***very strictly*** and basically only to avoid "***absurd***" consequences from the application of the normal rules. In Denmark, exceptions to the right of data subjects to be informed, or to be given access to his or her data, are allowed in view of "**overriding *vital* private interests**" - which also suggests a strict test.

The law in Austria allows for exceptions when "**necessary**" to protect the ***data subject*** him- or herself (which is in accordance with the Directive), or if the interests of the data subject are "**overridden by the *legitimate* interests of others**" (which seems to fall short of the "necessity" test). The German law allows for exceptions to protect "***confidential sources***" or "***commercial interests***" of the controller, on the basis of "**balance**" tests which also appear to fall short of the Directive's requirement of "necessity". The law in Spain says that **public-sector controllers** may refuse to comply with access requests etc. if the is "**necessary**" to protect ***private interests***, but is unclear as to whether **private-sector controllers** can refuse such requests, or when. The Swedish law grants private-sector controllers the right to refuse access requests etc. "in corresponding cases as under the Secrecy Law". That latter law

provides for a very limited number of relevant exceptions, each of which was introduced after a careful balancing of interests by the legislator.

The law in the UK contains a series of **more specific exception clauses**, which reflect the view of the legislator on how the balance between conflicting interests must be struck in particular contexts. Thus, as already mentioned above, at 9.1, under one of these provisions access can be denied to a data subject if this would involve disclosure of ***information on another person*** and it is "***reasonable***" to refuse access for that reason. Under another provision access can be denied to "***confidential references***" given about job applicants etc. The law also allows controllers to refuse access to personal data used in "***management forecasts***" or ***–"planning***" and ***negotiations with the data subject***. In Ireland, the law (apart from the - excessively wide - restriction on subject access concerning data on other persons, discussed above, at 9.1) also contains some **more particular exceptions to subject access**, 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); matters which are or would be covered by ***privilige*** in court proceedings; ***back-up data***; and ***data used solely for statistics and research*** (provided the data are not used for any other purpose and the results are not made available in identifiable form). These exceptions are again to be left unchanged in the proposed new (amended) law.

All in all, **the laws therefore vary considerably** in the ***scope*** of the exceptions and in the ***tests*** applied (which are often quite vague). Although they generally agree on the need for exceptions to protect the data subjects or others (including controllers), there are therefore still **wide divergencies** between the laws and practices of the Member States.

However, with regard to the use of CCTV-monitoring there is **greater concensus** on the basic principles and, in some countries at least, **clearer guidance** on the detailed application of those principles.

In all the Member States it is clear that **sound- and image data** captured by such systems are subject to the law - that is: that they constitute "***personal data***" - whenever they "can be" linked to an identifiable individual.[98] As noted above, at 2.1, this is indeed expressly stipulated in the Luxembourg and Portugese laws. There is the general issue of when this is the case, i.e. of whether the concept of "identifiability" is absolute or relative, as discussed above, at 2.1 - but as such that issue is not specific to CCTV-data. In any case, it is clear that in all the Member States which take the "relative" approach to this issue, sound- and image data caught by TV cameras will be regarded as subject to the law whenever they are linked to individuals, in particular through ***face-recognition software***, but also of course if the person monitoring the TV screen in question ***knows***, and can ***recognise***, the individuals concerned. In spite of a reference to "physical media" in the Spanish law, that law too applies to both transient monitoring and the recording of video images. In Denmark, as we have seen above,

[98] In the sole case in which the matter was addressed in Ireland (under the current, pre-implementation law), the data protection authority used rather cautious language: "*In recent times, several parties have sought advice on the privacy implications of the introduction of CCTV systems and have asked if such systems are regulated by the Data Protection Act. My advice has been that* ***developments in both technology and the law suggest that such systems will shortly be governed by data protection legislation if this is not already the case****. Accordingly it would be prudent for those responsible for the introduction of CCTV systems to consider and apply the principles underlying the Data Protection Act from the outset.*" However, that was several years ago (in 1996) and the authority would now clearly take the same view as his colleagues in the other Member States, especially under the proposed new (amended) law.

at 2.1, the installation of a webcam in a pub was held to involve processing of personal data because someone (anyone) might recognise the individuals whose images are disseminated on the 'Net.

It is accepted in principle in all the Member States that, when CCTV data fall under the law (as just discussed), the controller of the processing of those data must comply with all the relevant requirements of the law in question, e.g.: there must be a "***specific, legitimate purpose***" to the processing; the processing must be based on one of the "***criteria for lawful processing***" (such as "unambiguous consent" or the "balance" criterion); the data subjects (i.e. any "identifiable" person whose data are caught on the system, even if only transiently) must be ***informed*** of the data collecting and given the possibility to exercise their ***rights***; the processing must be "***notified***"; etc. And of course, such processing will be subject to **supervision** by the relevant Data Protection Authority. In Belgium, there is one court judgment relating to the use of secret TV-monitoring to catch a stealing employee (who was reasonably suspected of such theft), but little guidance otherwise. In Portugal, it was held that video surveillance or –monitoring inherently involved the processing of (particularly) "private" matters - and that this therefore must always be considered as processing of "sensitive data" (cf. above, at 7.1). This ruling had important implications (as discussed above, at 3.4) and also meant that certain formalities had to be observed (in that **transient monitoring** must be ***notified*** to the data protection authority, while **recording** requires the authority's ***prior authorisation***). However, it did not as such clarify the conditions under which such processing (such surveillance) could take place.

However, in a number of countries **much more detailed** rules or **clarifications in individual cases** have been issued. The Luxembourg law includes a special definition of "**surveillance**" which includes (but is not limited to) CCTV-data:

> "'**surveillance**' [means] all actions involving the use of technical means aimed at detecting, observing, copying or recording movements, images, words, writing, or the location of an object or person, whether stationary or moving."

The Luxembourg law goes on to set out two special (and detailed) provisions on "***processing for the purpose of surveillance***" and "***processing for the purpose of surveillance at work***". A **special law** has been adopted on the subject in Sweden (which is currently being reviewed); and a **special provision** on the matter has been included in the law in Germany, where it is also said that a future law on data protection for employees will address the issue further. In Finland, the issue is already addressed in exactly such a law, In Denmark too, video surveillance is subject to a **special law**, which stresses the need for CCTV camera operators to ***inform*** the public about their use, but to this has been added more detailed, additional guidance from the data protection authority. In Spain, the use of video surveillance by law enforcement agencies has been regulated in a special law. In the Netherlands, there have been decisions on the use of CCTV cameras on the street, in banks, in (and outside of) brothels, and in toilets in casinos, while in Greece, detailed general guidance has been issued by the data protection authorities.

In the UK, the Local Government Information Unit produced a **model code** for CCTV systems operated by local government bodies ("A Watching Brief – A Code of Practice for CCTV") as long ago as 1996. Since then, an extensive range of **further advice** on legal and technical aspects of CCTV has been issued by the UK authorities and private bodies: an

overview of these documents is attached. In addition, the UK data protection authority commissioned a report on **data protection in the workplace**, which also covered the use of ***CCTV cameras in that environment***: an excerpt from the relevant section is also attached (the latter report has, however, not yet led to further official guidance or regulation). In the absence of more formal regulation, the Irish data protection authority recommended the UK advice for use in that country in his remarks in the 1996 case, mentioned earlier; and he also broadly follows the further advice provided in the UK, e.g. in his discussions with the Irish police and in the drawing up of guidelines for community-based CCTV systems.

In France, a law on the use of **CCTV systems in *public places*** was adopted as long ago as 1995. This law established a **special supervisory authority** for such systems, in addition to the general supervision by the data protection authority, the CNIL. The latter has furthermore given very extensive attention to the wider matter of "**cybersurveillance**" as well as **CCTV-monitoring** in the ***workplace***.[99]

This is not the place to discuss each of the above-mentioned sets of rules or their practical application in full. However, I attach to this section a copy of one set of rules, the "*Directive on Closed-Circuit Television Systems*" issued by the Greek Data Protection Authority in 2000, which in spite of its concise form shows the very precise matters that can be - and should be - applied in this respect. As far as practice is concerned, I may refer to what I believe to be the most extensive study available: Norris & Armstrong: The Maximum Surveillance Society - the Rise of CCTV, Oxford & New York, 1999. This book includes (in Part II) a detailed report on the **actual practice of CCTV surveillance operators**, drawing on a two-year study of the operation of three CCTV control rooms, funded by the (UK) Economic and Social Research Council. It covers matters such as: external (legal and statutory) regulation; internal regulation in the form of codes of conduct; a chapter on the kinds of people employed in the industry; and incisive reports on questions including: "*Who was Surveilled and Why?*" (the answer to which is that "*both suspicion and [police] intervention are socially constructed*" and are selectively targetted on "*social groups which [the operators] believe most likely to be deviant*", which leads to "*over-representation of men, particularly if they are young or black*").

Here, certain **general features** of relevant regulation may be noted. Foremost of these is the need to ensure **openness** with regard to CCTV use, and to ***limit*** the risk that such technology is used in a way which unduly interferes with individual privacy. The rules generally (but not in Luxembourg) distinguish between ***transient*** monitoring (i.e. without the data being recorded) and ***recording*** of CCTV images. In this respect, the German law lays down a **dual necessity** test: cameras may only be *installed* if ***necessary*** for a legitimate purpose (which can be an overriding public interest or the protection of a person's house), but even then the data may only be *recorded* if there is a ***separate need*** to retain the data. The Finnish law is more complex but effectively makes a similar distinction, while the French law requires **prior authorisation** for the use of ***face-recognition*** software. In Spain, the Data Protection Authority has ruled that if CCTV-data used for the control of access to buildings are retained they must be erased within **one month**.

---

[99] See, in particular, the extensive section on the matter in the authority's most recent (22nd) annual report (covering the year 2001). The matter was also already addressed in the 12th, 15th, 20th and 21st Annual Reports of the CNIL.

The rules in Greece, Germany, Luxembourg, the UK and elsewhere stress the need for companies etc. who use CCTV cameras to **make this known**, e.g. through ***labels*** stuck on, or placed near, such cameras, which should ***inform*** the public or the selected persons being monitored of the identity of the controller and if necessary of the purpose of the surveillance. **Secret surveillance** is only allowed if the consequent surreptitious collecting of personal data is justified in terms of the law, i.e. if it fulfils one of the exceptions or derogations envisaged in Art. 13 of the Directive (as reflected in the relevant national law), as discussed above, at 10.3.

As far as the use of CCTV cameras in the **workplace** is concerned, the rules in Finland, France, Luxembourg (and elsewhere) stress the need to ***inform*** the employees in question, and add to this a requirement that the relevant **Workers' Council** be consulted both on the need for such surveillance in the first place, and on the rules to which the cameras and the data are put. It may be noted that the UK report on data protection in the workplace also approvingly refers to an example of workplace consultation. However, there is **no full unanimity** on the issue. Thus, the UK report just mentioned quotes (without dissent) the view of an employment lawyer that "***if employees know that they are being filmed and do not resign in response to this action, an employer is likely to succeed in arguing that the employees impliedly 'consented' to its actions by staying at work*** and, further, that they have not suffered any financial loss." This contrasts with the stipulation in (e.g.) the Luxembourg law, that "***the consent of the data subject [i.e. an employee] does not render processing [for the purpose of surveillanced at work], instigated by the employer, lawful.***"

By and large, the differences in these rules are unlikely to affect the Internal Market: CCTV systems are almost always used purely within one physical location, situated within one country (although I was informed of a system through which a company in the Netherlands controlled bridges in Poland). At most, it may mean that companies operating in different countries may have to adopt different rules for their different establishments - although even that could be avoided if they were to conform to the strictest legal regime concerned.

ATTACHED: Overview of advice provided in the United Kingdom on the use of CCTV systems by public bodies;

ATTACHED: Excerpt from: Robin E J Chater, The Uses and Misuses Of Personal Data In Employer / Employee Relationships, PPRU Study (Draft) Report, commissioned by the UK data protection authority, January 1999;

ATTACHED: "*Directive on Closed-Circuit Television Systems*" (Directive 1122 of 26 September 2000), issued by the Greek Data Protection Authority.

- o – O – o -

ATTACHMENT TO SECTION 10.4 (protecting the rights of data subjects and others): Overview of advice provided in the United Kingdom on the use of CCTV systems by public bodies.

Document	content	Order point
"***CCTV- Looking Out for You***" Home Office, 1994	Advice about setting up a CCTV system	020 7273 3037
"***CCTV Operational Requirements Manual***" PSDB	Advice on system requirements	01727 865051
"***User Guide to CCTV Systems Performance***" British Security Industry Association	Advice on systems performance. (Update expected for late Autumn 1999).	01905 21464
"***A Watching Brief – A Code of Practice for CCTV***" Local Government Information Unit, 1996	A model code to promote recognised standards and safeguards, reflecting the data protection principles. Widely adopted by CCTV operators.	020 7608 1051 Cost £75 (ISBN 1 8979 57 19 X)
"***The Data Protection Act 1998 – An Introduction***" The Data Protection Registrar, 1998	Advice on the application, requirements and scope of the 1998 Act.	01625 545745 www.open.gov.uk/dpr/dprhome.htm
"***Code of Practice and Procedural Manual for operation of CCTV***" CCTV User Group, 1999	Prepared by CCTV User Group Standards Committee to safeguard integrity of any CCTV system whilst ensuring the right to privacy is not breached.	01525 240737
"***Code of Practice for the Management and Operation of CCTV***" BSI British Standards Institution, 1999 (due Winter 1999)	Designed to supplement introductory advice on the Data Protection Act 1998. Gives recommendations on the operation and management of CCTV	020 8996 9000
"CCTV: making it work- Recruitment and selection of CCTV operators" 8/98 PSDB	Advice on selection process, competences, assessment methods, generic details on operator tasks.	01727 865051
"CCTV: Making it work "Training Practices for CCTV operators" 9/98 PSDB	Advice on training operators who monitor public areas. Focus on competences, training needs, good practice and designing evaluating training.	01727 865051

Source: the **Crime Reduction Website** (launched in July 2000 by the UK Home Secretary and "aimed at practitioners to help them achieve and sustain reductions in crime and disorder."): http://www.crimereduction.gov.uk/

ATTACHMENT TO SECTION 10.4 (protecting the rights of data subjects and others): EXERPT FROM: Robin E J Chater, The Uses and Misuses Of Personal Data In Employer / Employee Relationships, PPRU Study (Draft) Report, commissioned by the UK data protection authority, January 1999

The Use Of Closed Circuit Television (CCTV)

There are a number of data protection issues associated with the use of digital imaging equipment in the workplace. The most important of these are the:

* location of CCTV cameras
* use of covert monitoring techniques
* existence of third party images on video tapes
* use of surveillance other than for genuine security purposes
* security of images once they have been recorded
* duration that CCTV tapes should normally be held by employers and/or their agents
* legality of decisions based solely on video material

Section 29 of [the UK data protection law] sets out an important exemption from much of Data Protection Principle 1 and general subject access rights the processing of personal data for 'the prevention or detection of crime and the apprehension or prosecution of offenders'. This, however, is not a licence for security operations to stand outside the confines of The Act. Not all security problems relate to the 'criminal law'. Video evidence is normally admissible in civil proceedings and amongst the key purposes which suppliers frequently use to justify surveillance at work are health / safety monitoring and such day to day management concerns as the use of car park spaces.

According to the employment barrister Michael Ford 'if employees know that they are being filmed and do not resign in response to this action, an employer is likely to succeed in arguing that the employees impliedly "consented" to its actions by staying at work and, further, that they have not suffered any financial loss'.

In Guy's hospital the public sector union UNISON has threatened industrial action over the placing of surveillance cameras in locker rooms, whilst the GMB union has expressed concern during this study about the increasing reliance in the retail sector upon 'mystery shoppers' whose purpose is to monitor the competence of sales staff. On the other hand, in local government and higher educational institutions surveillance at work has not yet become an issue because the focus of security operations is usually on external locations with the sole object of detecting intruders. The monitoring of construction sites is now commonplace and UCATT has cited a recent industrial action on the Jubilee line where security data was used in reverse of its usual application to prove that union members could not have been in the vicinity of a suspected act of vandalism.

One of the largest multiple retailers revealed during the course of this study that some time ago their security department had attempted to counter suspected staff fraud by the use of covert surveillance cameras. The human resources department had questioned the invasive nature of the exercise and decided that the organisation should develop a more surveillance policy. They now consult a panel of staff representatives about the positioning of all security equipment.

The British Securities Industry Association has recently encouraged the establishment of a committee to draw up a new British Standard for the handling of CCTV video material. Because modern digital imaging systems have the capability to fabricate a video and wrongly implicate an individual in a crime it is essential that the integrity of actual CCTV images is maintained through procedures which can be readily subjected to an audit trail.

ATTACHMENT TO SECTION 10.4 (protecting the rights of data subjects and others) – Greek Data Protection Authority Directive on CCTV systems

HELLENIC REPUBLIC
DATA PROTECTION AUTHORITY

Address: Omirou 8
105 64 Athens, Greece
Telephone: +30 1 3352604-5
Fax: +30 1 3352617

Athens, 26.09.2000
Ref. No.: 1122

D E C I S I O N

SUBJECT: DIRECTIVE ON CLOSED CIRCUIT TELEVISION SYSTEMS

On 07.09.2000, Data Protection Authority convened at a regular meeting on its premises. Present at the meeting were the following: President, Mr. K. Dafermos; Members, Messrs. S. Lytras, E. Kioudouzis, N. Alivizatos, P. Pagalos, A. Papahristou and V. Papapetropoulos;

Mrs. K. Karvelli performed secretarial duties at the meeting.

Upon discussing the issue of closed circuit television systems, the Board issued the following directive, according to article 19 par.1 section a of Law 2472/1997:

The Data Protection Authority

WHEREAS:

1. According to article 2 par. a of Law 2472/1997 and EC Directive 94/46, audiovisual data, when relating to individuals, are considered to be personal data,

2. Storage and transmission of image of an individual, recorded by a fixed closed circuit television, operating on a regular, continuous or permanent basis, outdoors or indoors, such as on streets, squares, stations, ports, stadia, in banks, stores, theatres, cinemas, or public transportation means, constitute processing of personal data, in the terms of article 2 par. d of Law 2472/1997,

3. The mere recording of such an image by a closed circuit television, without it being stored or further processed, does not exempt the Controller from the obligation to notify to the Data Protection Authority said recording and inform the data subjects accordingly, in the terms of articles 6 and 11 of Law 2472/1997,

4. According to article 19 par. 1 section a of Law 2472/1997, the Data Protection Authority shall issue directives for the purpose of a uniform application of the rules pertaining to the protection of individuals with regard to the processing of personal data,

Decided upon the issuance of the following directive:

DIRECTIVE

on

"Processing of personal data through closed circuit television systems"

Article 1

Conditions of processing

1. Recording and processing of personal data by a closed circuit television operating on a regular, continuous or permanent basis is prohibited, because it may infringe on individuals' right to privacy.

2. Exceptionally, such a recording (on a regular, continuous or permanent basis) and such a processing are considered to be lawful, under the terms and conditions provided for in Law 2472/1997, without prior consent of the data subject, when the purpose of processing is the protection of individuals or goods or the regulation of traffic.

A. The criteria for the lawfulness of processing are the following: a) the principle of necessity, in terms of which the processing is allowed if its purpose cannot be achieved by any other equally effective but less irksome for the individual means (such as detectors at the entrance and exit of indoor premises), and b) the principle of proportionality, according to which the legitimate interest of the Controller must prevail over the rights and interests of the individuals to whom the data relate, provided that their fundamental rights are not violated.

B. Data collected by a closed circuit television shall be adequate, relevant and not excessive in relation to the purpose for which they are to be used each time. Therefore, the locations where the fixed video cameras shall be installed, as well as the way of recording, shall be such so that no more information than is necessary for the purpose pursued is recorded. For example, if the closed circuit television of a store or a bank aims at preventing a theft of goods or a robbery, data collected shall not be such so that they may be used to monitor the behaviour or the efficiency of employees.

C. In open spaces, video cameras shall be installed in such locations so that they do not overlook the entrance or the interior of private residences.

D. Data collected shall be accurate. However, 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 for face or vehicle recognition.

E. In the event that the collected data are stored in any way, they shall not be retained for a longer period of time than that required for the purpose pursued and, in any case, no longer than 15 days. In exceptional cases, data may be held for more than 15 days upon special permission of the Data Protection Authority.

F. Special attention shall be given to security measures taken against unlawful processing for as long as data are retained. This means that the Controller will have to give special consideration to, amongst others: i) security of and access to the central control room as well as the storage room where the recorded material is kept, ii) selection and recruitment of appropriate personnel, iii) ongoing training in data protection and privacy issues, and iv) respect, in general, of the rules provided for in Law 2472/97.

G. If the purpose of processing is to prevent or repress crime, the transmission of data shall be made exclusively to the competent judicial or law enforcement authorities. Transmission of data to mass media is allowed only in exceptional cases and upon special permission of the Authority, in the event that the public's assistance is deemed absolutely necessary for the recognition of individuals involved in a criminal activity, without nevertheless ignoring any possible objection of the victim.

Article 2

Special obligations of the Controllers

A. The Controller shall notify to the Authority the establishment of a closed circuit television system as well as the beginning of data processing, in the terms of article 6 of Law 2472/1997. Specifically, the Controller shall state clearly the purpose of data processing, the category of data to be collected, as well as any recipients to whom such data may be communicated.

B. Any individual, or vehicle, about to enter an area monitored by a closed circuit television must be notified accordingly by the Controller in a comprehensible manner. For this purpose, discernible signs shall be placed in an adequate number and in visible spots, notifying the public of the existence of cameras on the premises. These signs shall also identify the owner/operator of the system, the purpose for which such recording is taking place, the name of the person with whom individuals may communicate in order to exercise their rights under Law 2472/1997, and in particular the "right to access" and the "right to object". Said notification may be carried out by any other means provided for in the Regulatory Act 1/1999 issued by the Data Protection Authority.

C. The Controllers' attention is drawn to the fact that the Data Protection Authority may exercise, at any time, any necessary control, even *ex officio*, and to impose administrative sanctions to the offenders, as provided for in Law 2472/1997.

D. It is self-evident that in order to collect and process sensitive data, such as, for example, in hospital or insurance funds premises, prior permission of the Data Protection Authority is required.

E. The present directive is also applicable to closed circuit television systems already in operation. Therefore the Controllers are obliged to comply with the provisions hereof in due course and no later than January 21st, 2001.

To be published in the Official Gazette (Article 19 par. 8 of Law 2472/1997).

For the Data Protection Authority

The President

Konstantinos Dafermos

11. confidentiality and security

introduction

Article 16
Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17
Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

summary of findings

The laws in all the Member States stipulate the data security- and confidentiality requirements set out in Arts. 16 and 17 of the Directive, often in terms identical or close to those used in those articles. They thus all stipulate, in only slightly varying terms, that "**appropriate technical and organisational measures**" must be taken, and that the appropriateness of these measures is to be determined by reference to the ***risks*** represented by the processing, the ***nature of***

the data, etc. Some laws include some **additional stipulations**, e.g. that within the organisation of the controller access must be limited on a ***need-to-know*** basis (Belgium); that staff must be ***instructed in all relevant (data protection) laws and –rules*** (*idem*); or that public authorities must make provision for the ***destruction of data which can be of use to an enemy, in case of war*** (Denmark). Two cases from Ireland may illustrate how quite far-reaching consequences may flow from the confidentiality- and security requirements (and that action to remedy earlier failures may be quite costly):

> CASE EXAMPLE: A line manager in a company had created a file, setting out performance ratings for staff under his supervision. However, the "access permissions" on this file had inadvertently been set to allow numerous people outside of his management team to read it. The data protection authority held that this contravened the security requirements of the Irish data protection law and that the resulting dissemination of the file to staff members who should not have been authorised to have access to the file amounted to an incompatible disclosure of the personal data. The company put in place an immediate training programme in IT security, together with refresher programmes; destroyed all remaining hard- and soft copies of the file, with all company systems swept to confirm this; reissued HQ policies on data security; and reviewed and aimed to publish its standards on the holding of sensitive data.

> CASE EXAMPLE: A financial institution in Ireland had issued a type of debit card (called a "Laser card") aimed at being used in shops for cashless transactions. The customer's home address details were included in the information in the magnetic stripe on the card, but were supposed to be readable only by automated lodgement machines (for which this information was a legal requirement). However, some other terminals had their software upgraded to a new version, with the unintended result that the address details were read by the terminal and printed on the receipt. The Irish data protection authority considered this to constitute a breach of the security requirements, which had led to inappropriate disclosure. The company omitted address details from new cards unless the cardholder needed to avail him- or herself of lodgement facilities and took technical measures to ensure that, to the extent that such data were retained on the card, they could not be (read and?) printed by the relevant terminals; the Laser cardholders affected by the problem were identified, and a roll-out of replacement cards was initiated; and the company took measures to ensure that it would be consulted on future upgrades to the software.

All the laws (as concerns Ireland, the proposed now (amended) law) also stipulate that controllers have a duty to select a **processor** who offers sufficient ***guarantees of reliability and competence*** (or "commitments and guarantees", as it is put in the German law), and several laws (e.g., the ones in Germany and Italy) stress that the controller must ***actively ensure*** that the processor does in fact act properly, i.e. that the controller must ***inspect*** the work of his agent, and that the controller is ***liable*** for the (wrongful) actions of the controller. The

Finnish law only stipulates this with regard to ***professional processors***, while the French law stipulates, more generally, that the engagement of a processor does not absolve the controller from his duty "to ensure that [the security measures required by the law] are adhered to."

Most laws also specifically stipulate (again in accordance with the Directive) that processors must process personal data **only as instructed** by the controller. Several (e.g. Belgium, Denmark, the Netherlands) expressly specify as an **exception**, processing (other than as instructed) which the processor may be required to carry out ***by law*** (this would apply, e.g., to the compulsory handing over of data tapes to the police, in accordance with the relevant legal requirements) - but this exception can of course also be read into the other laws. The German law in this respect adds that a **processor must inform the controller** if he (the processor) believes that the instructions given to him by the controller are ***contrary to the law***. The law in Finland only expressly refers to the duty (also stipulated in the other laws) of all who process data (whether working directly for the controller or employed by a processor) to maintain **confidentiality** in respect of any personal data they have access to.

The laws also all stipulate that the arrangements between the controller and the processor must be set out in a (**written**) **contract** - but only a few (Belgium, the Netherlands, and the proposed new (amended) law in Ireland) add expressly that other, ***similar (recorded) "legal acts"*** or ***other (e.g. electronic) means of recording*** the arrangements, or "***another equivalent form***" can also suffice. The proposed new French law merely refers to a "***contract***", without reference to its form.

The UK data protection authority has expressed a concern that the formal requirements of the Directive in this regard may be excessive with regard to (say) the processing of a membership list of a small local football club on the club's behalf by a member (but the UK law nevertheless remains faithful to the Directive in these requirement). The stipulation in the Finnish law limiting the liability of processors for wrongful actions of to "professional" ones, noted above, can be seen as an expression of that same concern.

On the question of which national data security rules apply, the Directive contains an exception to the normal rules, in that it says that controllers must comply with their **local legal requirements** (rather than with the requirements of any other national law which may apply to the processing as a whole). This is repeated expressly in the Dutch law - but the Finnish law says that the processor must ***also*** comply with his local legal requirements (which suggests that the processor must comply with ***both*** the security requirements of the

country where his principal [the controller] is based, ***and*** with his own local requirements.

On the question of domestic rules, the law in Germany *used* to be quite specific about security requirements relating to various aspects of processing operations, by requiring, point by point:

- access control of persons;
- data media control;
- data memory control;
- user control;
- personnel control;
- access control to data;
- transmission control;
- input control;
- instructional control;
- transport control; and
- organisational control.

These stipulations were quite influential: references to some or all of these specific control elements can be found in laws, rules or advice on data security in many countries (e.g., in the Luxembourg law with regard to processing of all personal data, or in the special security measures stipulated with regard to the processing of sensitive data in the Portugese law). However, the German law itself has moved away from this specific list, in recognition of the emerging different data processing environment: it was felt that the above list was too much tailored to old-fashioned kinds of main-frame computers. The new law therefore itself only refers to "appropriate" measures. However, at the same time the data protection authorities and –experts in Germany have been trying to clarify how data protection can be ensured in the "information era". A working paper produced a few years ago thus first of all identified some **new main aspects** on which data protection should focus:[100]

- authority (the basis for providing access, e.g. a contract);
- identification and id-verification (to ensure access is only granted to authorised users);
- access-control;
- logging; and

[100] "*Datenschutzfreundliche Technologien*" (1997), paper produced by a working group made up of the Federal Data Protection Commissioner and several *Landes*-Commissioners, with input from the European Commission (then DG-XV) and the German Federal Office for information security.

- reporting (on use and access of the system).

The paper then discussed a series of **data-protection-friendly technologies**, with reference to the principles of "***data minimisation***" and "***as-soon-as-possible anonymisation***", i.e.:

- self-generated pseudonyms;
- pseudonyms for which the key is contained in a separate list;
- one-way pseudonyms;
- hash-keys;
- digital signatures;
- electronic certificates;
- blind digital signatures;
- biometric keys;
- the use of trusted third parties (in several ways); and
- identity protectors.

This theme was taken up again and further developed in the recent (2001) German report *Modernisierung des Datenschutzrechts* (Mondernisation of Data Protection Law). Here, it will suffice to note that the working paper and this report emphasise two matters of particular relevance to this Study: the need to start thinking about ***using technology*** **to ensure data protection** rather than regarding data protection as a means to ***counter*** technological developments ("*Datenschutz durch Technik*"); and the fact that the means to ensure data protection and data security clearly increasingly involve the use of **biometric data**, including ***sound and image data***.[101]

The French data protection authority, too, has long promoted the introduction of "**privacy-enhancing technologies**" or PETs and both works closely with industry and issues its own guidance, e.g. in the field of telematics, on-line access to data, encryption, biometrics, etc.[102] While welcoming such technologies, the authority is however also concerned that companies promoting such PETs offer products that afford real protection. In that respect, it is to be noted that the proposed new law in France allows the authority to express an "**opinion**" on the compatability of such products with the law. In effect, this means the CNIL will be able to give such products its "***seal of approval***" (or to withhold such approbation).

---

[101] For an extensive, insightful overview of the technologies and of the trends in data processing which will determine their use, see the research papers on "personal [i.e. identifiable] sound and image data" or PSID, prepared in connection with this study by Danny Meadows-Klue: *Trends in the PSID Data Explosion* and *Examples of PSID Technology*, London, 2002.

[102] See again, in particular, the latest (22nd) Annual Report of the CNIL (2001).

At a different level, the Swedish data protection authority has issued a useful **guide** on how controllers and processors should approach data security measures.[103] The guide clarifies the **organisational measures** needed to ensure security, starting from the need to draw up a ***security policy*** (which should also cover emergency procedures, back-ups, etc.) and to ***monitor*** processing, but also gives detailed **practical advice**, e.g. on the need not to write down passwords, or share them; to log off from a monitor if one leave's one's workplace; to ensure that screens cannot be read by unauthorised persons; etc. etc. And the guide discusses the various practical measures that controllers must take to deal with the various procesing steps, familiar from the previous German law (access control; media control; logging; etc.).

matters to be further clarified or addressed

The basic, somewhat abstract requirements of the Directive concerning data security and –confidentiality are generally re-stated in the laws of all the Member States. There is also a large measure of **general agreement** on the practical measures needed to adhere to them, often still related to the data processing elements addressed in the old German law (prior to implementation of the Directive).

Two matters should be noted. First of all, the question of **applicable law** arises in this regard in no less than ***three ways***. There is the question of which law applies to the processing to be carried out by the processor on behalf of the controller: this should be the law of the country in which the establishment of the controller is situated, in the context of the activities of which the processing can be said to occur (as discussed above, at 4). Then there is the rule that (in a departure from that general rule) the processor must adhere to his local law as far as the legal requirements concerning security and confidentiality are concerned. And then there is the law of the contract between the controller and the processor (which will cover, *inter alia*, the respective liabilities towards one another). It is not at all unthinkable that to each of these matters a different national law applies - which makes for a very complex relationship.

Secondly, the proposals put forward in Germany (and elsewhere) and which are aimed at relating the security and confidentiality requirements to the current and future technological (IT) environment should be taken into account in any revision of the Directive. Given that this is one area in which the practical requirements are largely common to all, irrespective of the details of the various

---

103 *Säkerhet för personuppgifter*, Data Protection Authority, Stockholm, 1999.

laws, this could be a very suitable area for further European co-operation and guidance. Cross-references can perhaps be made in a revised Directive (or in guidance issued under the Directive) to (developing) **European technical standards**, in much the same way in which this matter is largely left to domestic industry standards in the UK.

- o – O – o -

12. formalities

introduction

The system of "notification" and "prior checks", set out in the Directive, is not so much a system specifically designed by the drafters of the Directive as a reflection of the systems that were already in place. The aim of the system is to allow both the data protection authorities and individuals to have an overview of who processes what kinds of data for which purposes - i.e. to contribute to the essential need for "**transparency**" in the processing of personal data, without which such data cannot be effectively be protected, and without which data subjects cannot exercise their rights.

summary of findings

The matters to be notified under the national laws of the Member States usually include all the matters listed in Art. 19 of the Directive - but many national laws stipulate **further "notifiable particulars"**, such as information on the measures taken to inform the data subjects, and to allow them to exercise their rights *viz-à-viz* the controller, or information on the inclusion of the data in interconnected systems, etc., etc.

The laws in the Member States also all contain **exemptions** from the duty to notify with regard to certain processing operations. These usually include the most common, standard kinds of operations - such as ***salary administrations***, ***accounts records***, ***customer- and suppliers' records***, etc. - provided that those operations are carried out in accordance with certain **specified rules** or conditions. However, while these exemptions often apply to **very similar** (very similarly defined) **categories**, they are not ***identical*** - which means that some operations which would not have to be notified in one country would have to be notified in another. For instance, the exemption concerning ***membership data*** applies only to not-for-profit organisations in Belgium, but to any kind of association in Denmark. Then there are certain categories of processing operations which are ***exempt*** from notification in some Member States (e.g. processing of non-sensitive data for direct marketing purposes in Denmark), but not in others. And furthermore, the **conditions** for exemption (i.e. the standard rules to which exempt operation must conform) are ***different*** in the different Member States.

The same can be said with regard to the application of **more stringent formalities** such as the requirement of a "***prior check***" or the obtaining of a

prior "***opinion***" from the data protection authority, or similar requirements such as the issuing of a prior "***authorisation***" or "***permit***" by that body. Again, the **categories** for which such formalities are stipulated ***vary*** between the different Member States; and the specific **conditions** under which operations subject to such formalities are allowed also ***differ***.

A particular issue is the appointment of a **data protection official** on the lines envisaged in Art. 18(2) of the Directive. This institution is taken from German law, where such officials have played a major role in ensuring compliance with data protection rules and –regulations. Following the inclusion of the reference to such an official in the Directive, several Member States do now make provision for such an appointment - but in somewhat ***different situations*** and with somewhat ***different implications***. The **take-up** of this suggestion in practice also ***varies***.

Thus, the Dutch law makes special provision for the appointment of such an official, not just by individual controllers but also for **sectors**, and allows for notification to be made to such officials rather than to the data protection authority - but in practice ***few such officials have been appointed*** (at least in the private sector) because controllers feel it imposes burdens on them without bringing real benefits. In Belgium, the law envisages the appointment of a data protection official for a controller - or again for a **group of controllers** - as a condition which can be imposed in respect of processing operations posing specific **risks** to the rights and freedoms of data subjects (i.e. for which a "prior check" is required) - but the decree under which this can be required has not yet been issued. By contrast, the institution remains important in Germany, and there are plans to enhance it by setting ***standards*** for the training of such officials, and issuing ***diplomas*** to qualified and tested officials.

matters to be further clarified or addressed

Perhaps the most important thing that can be said about **notification** is that **everyone** - including in particular the data protection authorities - **agrees** that as currently operated in the Member States it ***serves little real purpose*** and ***takes up an excessive amount of resources***.

The point is that the details that are notified and laboriously recorded in the register of notifiable operations do not allow the data protection authorities, or persons consulting that register, to assess whether the processing by the controller in question is proper or even in accordance with the law. For that, even more information would be needed which it is unrealistic to expect. In practice, many domestic controllers still fail to notify their operations, while

non-EU controllers hardly ever register or inform the authorities of the appointment of a representative. To the extent that controllers do notify their operations, they make little effort to keep the particulars up to date. Data protection authorities do not very actively pursue non-registration (partly because they are aware of the limited usefulness of the system). And very few individuals actually consult the register. According to the UK data protection authority, the system may even have a ***negative effect*** on compliance, in that it suggests that controllers who have notified their operations act in accordance with the law, although in practice there is no certainty that this is the case at all.

There is widespread support on the part of authorities and controllers alike to **fundamentally review** the system of notification, and to ***reduce*** it significantly, for instance to a simple duty to register as a data controller, with a simple list of purposes for which the controller processes personal data (and perhaps a declaration that that processing conforms to the law). To this could be added a requirement that any controller must be able to produce forthwith (on request) the full details of his processing operations, including sources and recipients, categories of data used for each purpose, and of data subjects on whom data are held for each purpose, etc. More detailed notification, and further-going rules such as a requirement for a "prior check" or authorisation, should be reserved for "**risky**" operations.

The institution of the **data protection official** could be very useful but has not really taken roots outside Germany. Consideration should be given to ways in which the appointment of such an official could be made attractive to controllers, groups of controllers, or sectors. Merely exempting controllers from notification (as is now stipulated in the Directive) appears to be insufficient.

- o – O – o –

12. formalities – detailed findings

12.1 processing operations which must be notified and exemptions from notification

Article 18
Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

  - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

  - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

There are **quite different traditions** in the Member States with regard to notification (or registration) of processing operations, and the provision in the Directive, quoted above, reflects this. Some Member States rely heavily on notification (or indeed on prior authorisations or "prior checking", as discussed below, at 12.3), while others seek to minimise

such formalities. Following the Directive, all the Member States, in principle, require notification (or similar measures) of **all wholly or partly automated processing operations** (although they differ in the manner of notification, as noted below). In most Member States, notifications must be submitted to the national data protection authority. However, in Spain, filing systems established by **public authorities** need not be notified to the Authority: instead, the details of such systems must be ***published*** in the Official Gazette (*Boletin Oficial del Estado*) (or, if the system is established by an independent regional body, in the corresponding local Gazette), in the form of ***legislative provisions***. The Netherlands allows for notification of processing operations to an ***in-house data protection official*** (or indeed to a data protection official appointed for a certain ***sector*** by a trade association). The same is effectively achieved in Sweden and Luxembourg, in that the laws there stipulate that notification is not required ***if a controller has appointed an in-house data protection official*** of the kind discussed above - but the controller must inform the data protection authority of the fact that such an appointment was made, and the official must maintain an **in-house register** of processing operations, containing the same information as would otherwise have had to be notified; in Luxembourg, this **register** must be sent to the data protection authority. In Germany, such "in-house notification" is provided for in more limited circumstances (although, as noted below, at 12.3, in that country the in-house official can carry out the "***prior checks***" envisaged in the law). In Finland, controllers are similarly obliged to draw up their own, in-house "***specifications***" of their processing operations, but they must provide copies of them to the data protection authority (i.e. the drawing up of these specifications does not lead to an exemption from notification).

Some Member States extend the duty to notify processing operations (again, in principle) to ***all*** processing of personal data held in (structured) **manual filing systems**; some extend it to ***some*** **manual systems**; while many others provide for ***wide*** (albeit often ***conditional***) **exemptions**.

Thus, Denmark, Greece, Italy and Luxembourg in principle require notification of **all automated *and manual* processing operations** (in Luxembourg, of course subject to the exception in case of appointment of an in-house official). Finland extends the duty to any (i.e. also non-automated) processing which involves ***transfers of data to third countries***; the taking of ***fully automated "significant" decisions***; ***credit assessments*** and ***debt collecting***; ***market research***; ***staff recruitment***; and ***computer bureaux*** (i.e. professional processors); etc. – and the law in that country does not provide for any full or even conditional exemptions. And the law in Portugal extends the notification-requirement to ***non-automatic processing of "sensitive data" in order to protect the vital interests of the data subject or of another person*** (presumably, this only applies to controllers who regularly carry out such processing).

By contrast, the law in Austria **fully exempts** processing of ***published data***, ***data from public registers***, ***anonymised or pseudonymised data***, and data processed for the purpose of ***publication*** from notifications (even if they are processed by automated means), and also provides for **conditional exemptions** for ***standard operations***. Belgium, Denmark, France (already under the current law), the Netherlands and Sweden also make extensive use of the possibility to grant **conditional exemptions from notification** with regard to common forms of processing which comply with ***prescribes standards***, or they allow for a much **simplified form of notification** of such operations (basically consisting of a mere declaration to the

effect that processing in the category concerned conforms to these standards). A regulation issued under the UK data protection law also contains a number of **conditional exemptions**.

To give one extensive example of extensive reliance on "conditional exemptions": in the Netherlands, standard norms 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**.

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 60% of all processing notified to the data protection authority (although the numbers have been steadily falling, from some 54,000 in 1997 to just short of 30,000 last year). In Belgium, Denmark and Sweden too, considerable numbers of conditional exemptions from notification have been provided for, concerning processing relating to matters such as ***salary administration***, ***personnel administration***, ***accounts***, ***membership data***, etc. Notable are perhaps the exemptions from notification in Sweden with regard to ***data in running text*** and ***processing in accordance with an "approved" code of conduct***. The UK regulation, mentioned above, exempts just four types of processing operation: 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**. By contrast, Spain has not availed itself of the possibility to introduce "***conditional exemptions***" from notification for innocuous processing operations subject to simplified norms. The law in Luxembourg makes provision for the issuing of "**simplified norms**", adherence to which will exempt controllers from the duty to notify - but the law not yet having come into effect, the relevant "***directive***" has also not yet been issued. The same applies to the proposed new (amended) law in Ireland: it envisages exemptions on the basis of standard norms, and it is intended to use these widely, but the law not yet having been amended, the relevant Order has of course also not yet been issued.

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 their scope and specific detail. Even in respect of similar operations which, in different Member States, are subject to "***standard norms***" - such a ***salary- or membership administrations***, for instance - the norms are therefore **different**. Companies which want to harmonise such operations throughout their different entities in the EU will therefore often not benefit from such "simplified norms" or exemptions.

COMPLIANCE: In my earlier study on compliance with data protection law in the Member States, I noted that **notification is widely ignored**.[104] Thus, in the Netherlands, there was a ***massive discrepancy*** between the number of companies listed in the Companies Register and the number of controllers who notified their operations (the latter being just **2%** of the former). In the UK, a House of Commons select committee guessed in 1994 that about **one third** of controllers had failed to register; the data protection authority itself pointed out that by a different measures (a comparison with the Isle of Man), the figure might well be **two thirds**. In Germany, too, a system of central registration (notification) was considered "mere wishful thinking".

There is no evidence that this situation has significantly improved in the above-mentioned countries, or is any different in the other Member States: the percentage of registered controllers compared to the number of companies in a country (in my opinion, the best first indication of the level of compliance with notification) remains everywhere ***very low indeed***. One reason why notification is not more strongly pursued is that the data protection authorities in fact largely agree that the notified particulars are **a very poor indication of what goes on in practice** (even if they faithfully reflect what goes on, which is doubtful in itself, as discussed in the next section); and that it adds little if anything to compliance with the more onerous requirements of the laws. According to the UK data protection authority, the system may even have a ***negative effect*** on compliance, in that it suggests that controllers who have notified their operations act in accordance with the law, although in practice there is no certainty that this is the case at all.

Many of the authorities would therefore prefer to spend their resources on other measures which could contribute more effectively to compliance by controllers and to the protection of the interests of the data subjects. However, others believe that notification does have an "**educational**" **effect**, in that it forces controllers to examine their operations in the light of the law.

12.2 notifiable particulars and publication of particulars

Article 19
Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

[104] See the Interim and Final reports on a study into *Existing case-law on compliance with the data protection laws and principles in the Member States of the European Union*, jointly published by the Commission in 1998 as an Annex to the Annual Report 1998 (XV D/5047/98) of the Working Party established by Article 29 of Directive 95/46/EC.

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph I must be notified to the supervisory authority.

Article 21
Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide provide of a legitimate interest.

To the extent that they require notification, the Member States all list (at least) ***all the matters mentioned in Art. 19(1)(a) – (f) of the Directive***, quoted above; and they all of course also stipulate that if such aspects of a processing operation change, the change too must be reported. However, they **differ considerably** in their specification of ***additional notifiable particulars***. Thus, the law in Austria requires notification of details of any ***processor*** involved in the processing, and of the ***legal basis*** of any processing, or disclosing, or transfer (to the extent that such actions are based on such grounds). 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 data subjects***; the ***procedure for obtaining the data***; ***a description of the basic structure 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 and UK laws, 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.

COMPLIANCE: In my earlier study,[105] I noted that (according to an official in-depth review of the law in the Netherlands) the **quality of notifications** "***often fell considerably short of the expected standards***." The review in question concluded that:

> "The findings concerning compliance with the notification- and self-regulation duty are nevertheless in general disappointing. It is probable that these duties are **ignored to a substantial degree**, or otherwise ***complied with in the form***. It cannot be expected that an active enforcement policy on the part of the data protection authority can bring about (much) change in this." (emphasis added)

Again, there is no reason to believe that this has changed in the Netherlands or is different elsewhere: many controllers see the filling in of the notification-form as a "***one-off chore***", after which they can conveniently forget their obligations. As noted in my earlier study, this is only different in two types of organisations: where there is already an ***existing pattern of confidentiality and careful handling of personal data***, or where data protection rules otherwise meet an ***existing need*** of the organisation involved. Notification contributes little if anything to overall compliance with the laws.

---

105 See footnote 104, above.

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, the register contains both the ***notified particulars*** with regard to **private-sector controllers** and the ***published particulars*** of processing by **public-sector controllers** (as both listed above). However, the usefulness of these registers, too, is in doubt.

USE OF THE REGISTER IN PRACTICE: It is clear from the reports of the data protection authorities that **the register of notified particulars is relatively rarely used** (given the numbers of companies who have notified their operations, let alone the number of existing companies). 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.

12.3 prior checks

Article 20
Prior checking

> 1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.
>
> 2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.
>
> 3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

"**Prior checks**" or requirements that controllers obtain the "***prior authorisation***" of their national data protection authority, are the strictest form of control over processing operations. In accordance with the Directive, they are prescribed in the Member States for operations which (in the opinion of the authorities) pose "***specific risks***" to the rights and freedoms of data subjects. The system is most widely developed in France, where (under the current, pre-implementation law) all processing operations in the ***public sector*** must be based on a ***regulation***, adopted after the data protection authority has first given its "***advice***" - which in practice comes close to a "**prior check**". 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.

Otherwise, too, there are again (in spite of some overlaps) **substantial differences** between the Member States as concerns the kinds of operations for which they stipulate such prior formalities. Thus, in Austria, a "**prior check**" is required for processing of ***sensitive data***, processing for the purpose of ***credit referencing***, and processing involving ***interconnections*** between different databases. In Denmark, "**prior authorisation**" is also required for the processing by private-sector entities, of ***sensitive data*** and for processing by ***credit referencing***- and "***warning***"***-agencies***, ***staff recruitment agencies***, but the law adds to this processing for the keeping of ***legal information systems***, or for the ***transfer of sensitive data to third countries without adequate protection***. In Finland, only the first of these (processing of ***sensitive data***) requires a "**permit**", if the controller believes it must be carried out for a reason pertaining to an ***important public interest*** - but on the other hand, in that country, such a prior authorisation is required if the controller believes that the processing is necessary, otherwise than in an individual case, in order to protect the ***vital interests of the data subject***; if the controller believes that the processing is necessary in order to ***exercice official authority*** vested in the controller or a third person to whom the data may be disclosed; or indeed if the processing is to be based on a "***balancing of interests***" between the interests of the controller and the rights and freedoms of the data subjects. In Greece, **prior authorisation** is required for processing of ***sensitive data*** (even with the consent of the data subject!), for processing involving the taking of "***fully automated decisions***", as well as for the creation of "***interconnections***" between different filing systems. In Germany, processing of "***sensitive data***" and processing involving the taking of "***fully automated decisions***" requires a "**prior check**" - but in that country (uniquely) that check is, in the private sector, to be carried out by the ***in-house data protection official*** (rather than the supervisory authority). The Italian law too requires (***prior***) **authorisations** for processing of ***sensitive data*** in particular. In Luxembourg, the law requires a "**prior check**" for most processing of ***sensitive data***, including such processing with the ***consent*** of the data subject, and also including processing of ***sensitive data made public by the data subject*** (other than by the press: see above, at 10.1) or for ***research***; for ***surveillance*** (including CCTV and other monitoring at work); for ***iinterconnections***, processing in relation to ***credit referencing*** and ***processing of data for different purposes than for which they were collected*** (unless the data subject consents to the secondary processing). In the Netherlands, a "**prior check**" must be carried out for the use of an **identification number** for a different purpose than the one for which the number is intended, in order to match data with data processed by a different controller; for the **recording of data obtained through a controller's own observations** (which include both secret ***video surveillance*** and the ***capturing of Internet or intranet activities***) if the data subject is not informed of this; and for the **processing of data on criminal-legal matters** etc., other than by ***licenced detective agencies***. Portugal imposes a "**prior check**" on the processing of "***sensitive data***" on "***important public interest grounds***" and of ***data on criminal convictions etc.*** when this is ***necessary to pursue the legitimate purposes of the controller***; to the processing of personal data relating to ***credit*** and the ***solvency*** of data subjects; to the "***combining***" (***interconnection***) of personal data; and to the ***use of personal data for purposes which are different from the [specified purposes] for which they were collected***.[106] In Sweden, "**prior checks**" have, to date, only been stipulated with regard to ***processing of sensitive data for research purposes without the consent of the data subject*** (unless the research has been authorised by an "ethics committee"); and for "***processing of***

[106] The English translation of the Law, provided by the Portugese Data Protection Authority refers to "the use of personal data for purposes not giving rise to their collection" to translate the original Portugese text which reads: "*a utilização de dados pessoais para fins não determinantes da recolha*", but I take this to mean using of personal data for purposes not specified ("determined") at the time of their collection.

personal data concerning hereditary disposition derived from genetic investigation" (unles the processing is "governed by specific regulations in a law or a decree").

The law in Spain does not, in so many words, provide for "**prior checks**" for certain specified, "risky" operations. However, this is because, in effect, the data protection authority is given the possibility to subject **all** notified operations to a check of that kind. Specifically, the law stipulates that the data protection authority shall only enter the notified particulars in the register "if the notification meets the relevant requirements" (Sp: *si la notificacion se ajusta a los requisitos exigibles*). If the notification does not meet these requirements, in the sense that the controller has not provided all the required information, the authority may ask for the missing information; while if the notification fails to meet the requirements otherwise, the authority may take "***remedial action***". This includes the possibility of **ordering** controllers to bring their processing in line.

In Belgium, a "**prior check**" can be imposed on "risky" processing by means of a decree, but such a decree has not yet been issued, and in Ireland, too, the matter awaits adoption of the proposed new law.

COMPLIANCE: In some sectors, the obtaining of ***prior opinions*** or ***prior checks***, or ***prior authorisations*** or ***permits*** does become the norm, especially if (a) failure to obtain such a permit can lead to the loss of a licence and (b) the data protection authority puts in a concerted effort to convince those in the sector of the serious repercussions that failure to comply with the required formality may entail. It also helps if the sector in question is not too large. Thus, as again noted in my earlier study,[107] in the Netherlands, compliance with such a requirement by ***private detective agencies*** became the norm (although doubts remained over the extent to which such firms complied with the more substantive requirements of the law).

In general terms, the French data protection authority (which, as noted above, has the greatest experience with such a system) believes that it serves a **very useful** function - but the authority also notes that purely because of resource implications, such a system must by its nature be limited to selected areas or kinds of controllers. It could not, therefore, be general extended to the private sector, for instance. Indeed, one may add that one factor contributing to the positive experience with the system in France is undoubtedly the very fact that it operates in the public sector, in which there is (or at least ought to be) an ethos which should be responsive to the need to protect the interests of the citizen.

12.4 in-house officials

> [Member States may exempt controllers from notification where] the controller, in compliance with the national law which governs him, appoints a **personal data protection official**, responsible in particular:
>
> - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
>
> - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

[107] See footnote 104, above.

> thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.
>
> (Art. 18(2), second bullet-point, of the Directive)

The concept of the **data protection official**, appointed by a controller to ensure compliance with data protection requirements within the organisation of the controller, mentioned in the Directive in Art. 18(2), is of German origin. Already provided for in the 1977 Law, the institution was strengthened in the 1990 Law and retained in the 2001 Law.

According to the law, the appointment of such an official is **compulsory** for any company or organisation employing more than four employees in its automated personal data processing operations or employing more than 20 employees in manual personal data processing. Organisations which are subject to a "**prior check**", or which **"professionally" collect personal data with a view to their disclosure** (in identifiable or anonymised form), such as ***list brokers*** or ***market research- or opinion poll companies***, must appoint an in-house official, irrespective of the number of people they employ in the processing of personal data.

Anyone appointed as data protection official must have the required technical and technical-legal knowledge and reliability (*Fachkunde und Zuverlässigkeit*). He or she need not be an employee but can also be an **outside expert** (i.e. the work of the official can be ***outsourced***).[108] Either way, the official reports directly to the CEO (*Leiter*) of the company; must be allowed to carry out his or her function free of interference (*weisungsfrei*); may not be penalised for his or her actions; and can only be fired in exceptional circumstances, subject to special safeguards (but note that this includes being sacked at the suggestion of the relevant supervisory authority). The controller is furthermore required by law to provide the official with adequate facilities in terms of office space, personnel, etc..

The main **task** of the in-house official is to ensure compliance with the Law and any other data protection-relevant legal provisions in all the personal data processing operations of his employer or principal. To this end, the controller must provide the official with an **overview of its processing operations**, which must include the information which (if it was not for the fact that the controller has appointed an in-house official) would have had to be notified to the authorities (as discussed below, under the heading *notification*) as well as a list of persons who are granted access to the various processing facilities. In practice, it is often the first task of the official to compile this information, and suggest appropriate amendments (e.g., clearer definitions of the purpose(s) of specific operations, or stricter rules on who has access to which data). Once an official has been appointed, new planned automated processing operations must be reported to him or her ***before*** they are put into effect. The official's tasks also include **verifying the computer programmes** used in this respect; and **training the staff** working with personal data. More generally, the official is to **advise** the controller on relevant operations, and to **suggest** changes where necessary. This is a delicate matter, especially if the legal requirements are open to different interpretations. The Law therefore adds that the official ***may***, "in cases of doubt" contact the relevant supervisory authority However (except in the special context of a "prior check"), the Law does not make this ***obligatory***.

---

[108] This means of course that my use of the term "***in-house* data protection official**" is not always strictly speaking correct, but I will use it nevertheless to emphasise the fact that the official is appointed by and works for the controller, rather than an external state official.

The Dutch law too places particular emphasis on the institution of the **data protection official** (NL: *de functionaris voor de gegevensbescherming* or just *de functionaris*). Such officials can be appointed either by **a particular controller**, or - and this is unique to the Netherlands - by a (**sectoral**) **organisation** to which controllers belong.[109] The official must supervise the processing of personal data by the controller who appointed him (or her) or, if the controller is appointed by a sectoral organisation, the processing of personal data by controllers who belong to the organisation in question.[110]

This supervision must be aimed at ensuring compliance with the **law** and with any relevant ***code of conduct***. As noted above, the official (rather than the national data protection authority) can also be made responsible for receiving **notifications** of data processing operations carried out by the controller who appointed him, or by controllers belonging to the sectoral organisation which appointed him. As in Germany, the official must be a person with sufficient knowledge and trustworthiness. The national data protection authority maintains a ***list*** of all such officials. The official must be able to carry out his tasks in (relative) ***independence***, in the sense that the controller or sectoral organisation that appoint him may not give "directions" to the official, and in that the official may not be penalised for his activity. The official is subject to a special ***duty of confidentiality*** with regard to anything disclosed to him in connection with the lodging of a complaint. He (or she) must furthermore draw up an ***annual report*** of his (or her) activities and findings.

The appointment of an official does not affect the powers of the data protection authority, but in the Dutch system, the in-house or sectoral officials are nevertheless given important tasks. Indeed, the thrust of the system is that supervision over compliance with the Law and responsibility for the investigation of complaints etc. is left, in first instance, in the hands of these officials (where they have been appointed), with the national authority only intervening (or being called in) if the matter cannot be resolved in this way. The official's role is a ***delicate*** one. (S)he must be capable and willing to giving frank "advice" to his (or her) employer (or to the members of his\her employer's organisation) - but (s)he is not required to report improper activities. As the Explanatory Memorandum to the Dutch law puts it, the official is not "an extension of the [national authority]". However, if (s)he is in doubt as to the application of the law, (s)he *must* consult the data protection authority. Conversely, a controller or organisation who is unhappy with the advice from its own official, may still refer the matter to the State authority for clarification. In practice, it is hoped that the system will work in a (rather typically Dutch) co-operative, non-confrontational way. As it is put in the Explanatory Memorandum, the intention is to create an "easy working together" (NL: *een soepel samenspel*) of officials and authority (although the Memorandum acknowledges that conflicts cannot be excluded).

As noted above, at 12.1, the Luxembourg and Swedish laws, too, makes provision for the appointment of an **in-house official**, and exempt controllers who make such an appointment

---

[109] The Explanatory Memorandum claims that the possibility of providing for *sectoral* officials was expressly opened under the Directive at the request of the Netherlands - although there is no reference to this in any of the public documents relating to the various drafts, and although it seems somewhat at variance with the text of Art. 18(2) of the Directive, which refers to an official who is appointed by "the controller". Presumably, the concession to the Netherlands is recorded in the (unpublished) minutes of the Council of Ministers.

[110] Presumably, to the extent that the processing relates to the activity of the sector in question: some controllers, active in various sectors, could be subject to supervision by different sectoral officials.

from notification. However, other than the stipulations as to the drawing up of a "***register***" of processing operations, also already noted at 12.1, the details of such functionaries have not yet been spelled out in these countries. In Belgium, the law says that provision for an in-house official can be made in the special conditions under which processing posing "***special risks***" to the data subject may be allowed - but the decree in which this can be stipulated has not (yet) been issued.

No provision for an ***in-house official*** is made in the laws in Austria, Denmark, Greece, Finland, Italy, Portugal, Spain, or the UK, nor is the appointment of such an official envisaged in the proposed new (amended) law in Ireland. This does of course not mean that such an official cannot be appointed, but no special advantages or exemptions would be attached to such an appointment. The concept is also not developed in France - except that (as noted above, at 10.1) the law requires that **media enterprises** appoint a ***liaison person*** to maintain contact with the data protection authority.

EXPERIENCE IN PRACTICE: The experience with in-house data protection officials varies. In Germany, as noted above, it is regarded as a major means towards effective implementation of the law, and all major companies and authorities have made such appointment. In the Netherlands, a similar development was expected - but this has not really happened: only relatively few companies and organisations in the private sector have appointed such an official, and the appointment of a sectoral official is very rare. It is reported that this is because commercial bodies in particular see little benefit in such an appointment: they fear that the official will impose significant burdens, without providing tangible benefit. In Belgium, Luxembourg and Sweden the appointment of an in-house official is provided for, but has not yet been fully developed. In other countries, as also already noted, the legislator has not made any specific provision.

- o – O – o -

13. remedies, liability and sanctions

introduction

Article 22
Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23
Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24
Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the' provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

The existence and ready availability of effective remedies against unlawful or improper processing is of course essential to ensure both compliance with the law generally and enjoyment of the rights and remedies of data subjects in particular: *ubi remediem ibi ius*.

summary of findings

All the Member States allow for the possibility of data subjects seeking redress, and corrective action, though the **courts**. This includes the possibility for individuals (i.e. data subjects) to obtain **damages** by means of court action - although there are differences with regard to the ***kinds of damages*** for which aclaim may be lodged, and concerning the ***exculpatory provision*** specified in the Directive, often related to the legal culture of the country concerned.

For instance, under the Belgian and Portugese laws the controller is liable for compensation, unless he (the controller) proves that he is ***not responsible*** for the

event that caused the damage. The Danish law expresses the principle in somewhat more elaborate terms: a controller is liable for "any damage caused by the processing of data in violation of the provisions of this Act unless it is established that such ***damage could not have been averted through the diligence and care required*** in connection with the processing of data." In the Netherlands, the law says that the level of damages can be reduced depending on the extent to which the person being sued can be held ***accountable*** for the damage - but this latter matter is to be determined in accordance with the ordinary rules on full or partial liability. In Finland, France and Luxembourg, too, the ***ordinary rules*** on civil- and administrative liability apply. In Ireland, the current law already (in effect) makes any breach of the law tantamount to a **tort** (i.e. a ***civil wrong*** at common law), by stipulating that controllers and processors owe a "duty of care" to the data subject - but the law also clarifies that there shall be no liability concerning (alleged) inaccuracy "so long as the personal data concerned accurately record data or other information received or obtained by [the controller] from the data subject or a third party" and that fact is recorded with the data; the opposing view of the data subject is recorded; and a statement supplementing the data (i.e. setting out the opposing views of the data subject) is added.

In the UK, too, the law provides for compensation for damage caused as a result of any failure on the part of a controller to comply with the law - but the law is more restrictive as concerns "***distress***" (i.e. immaterial damage) than as concerns (material) ***damage***: the former can only be awarded if material damage has been proven. In practice, few claims are ever made: the case of Naomi Campbell, briefly set out above, at 10.1, is the first case ever in which compensation was awarded (although it could be the first of many, now that the possibilities of the law have been so widely publicised).

In practice, this means that there will be **differences concerning the scope of liabilities** borne by controllers, depending on which law is applied to the question of liability (which may not be the law that applies to the processing as such).

All the laws also contain extensive **penal provisions**, making most actions contrary to the data protection law a criminal offence, punishable by fines (or in serious, aggravated cases, e.g. when the offence was committed for gain, by imprisonment). They also all allow for the possibility of criminal prosecution of company directors etc. They adopt somewhat different formal procedures in this. 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, while other countries 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.

I will return to matters of enforcement in the final section in this report, section 16, where I will discuss the functions and powers of the data protection authorities in more detail. I will therefore also leave the question of *matters to be further clarified or addressed* to that section.

- o – O – o-

14. transnational issues (ii) - cross-border transfers

introduction

As noted above, at 4, transnational issues are of course of special importance to the Internal market. In particular, as is noted in the 3rd Preamble to the Directive:

> "the establishment and functioning of an internal market in which, in accordance with Art. 7a of the Treaty, the free movement of goods, services and capital is ensured require ... that personal data should be able to flow freely from one Member State to another ..."

Apart from trying to ensure - rather unsuccesfully, as we have seen - that there are no (positive or negative) conflicts between the laws of the Member States (as discussed in that earlier chapter), the Directive therefore also stipulates that "***Member States shall neither restrict nor prohibit***" the **free flow of data** between them for reasons of data protection (Art. 1(2)).[111]

And in order to avoid avoidance of the rules, the Directive also tries to ***harmonise*** the Member States' approach to **transfers of personal data** from their territories (i.e. from the territory of the Community) ***to other*** (so-called ***"third"***) ***countries***. This section reports on the findings of the study in these latter two respects: on the rules in the Member States concerning intra-EU data transfers (below, at 14.2) and on the rules concerning transfers of data to "third countries" (below, at 14.3). However, as in chapter 4, it was again necessary to note the (different) ways in which the Member States treat the non-EU EEA States (*Iceland*, *Liechtenstein* and *Norway*), also in this respect (below, at 14.1).

summary of findings

The study found that only three Member States expressly pronounce the **freedom to transfer data to other EU countries**, stipulated in Art. 1(2) of the Directive, while only one of these (correctly) limits it to matters ***within the scope of Community law***. The laws in most other Member States merely ***imply*** the freedom to transfer data to other EU Member States, by not subjecting such transfers to the restrictions which they *do* impose on transfer to non-EU (or non-EEA) States, but extend this implied freedom to matters both ***within and***

[111] The other stipulation in this Article (i.e. in the first paragraph of Art. 1), to the effect that the Member States must ensure a high level of data protection by implementing the Directive, is in a way merely the *conditio sine qua non* for the creation of the "free zone" for data transfers announced in the second paragraph (as is also clear from the text omitted from the words of the 3rd Preamble, quoted above).

without the scope of Community law. Of these, four extend this (implied) freedom to transfers to the **non-EU EEA States**, while another four limit it to the **EU States**. The law in one country is ambiguous in this respect.

Just as with regard to the question of "applicable law", discussed at 4, the ***uncritical application of a basic rule in the Directive (here: the stipulation of unimpeded data transfers within the EC) to matters not subject to the Directive*** can lead to **serious constitutional problems**, if the laws in the Member States concerned are seen as authorising unimpeded data transfers from Member States with a high level of data protection to Member States which, in the non-Community area within which the transfer takes place, do not provide the same, or an "adequate" (or perhaps not even any) data protection. As illustrated in the detailed findings on these matters, set out below, at 14.2 (with reference to anti-terrorist measures being introduced at the European level after the 11 September 2001 attacks on the USA), these issues are likely to arise, in particular, in connection with sensitive "Third Pillar" inter-governmental activities - but they may involve the use of data originating from "First Pillar" activities by citizens and residents of the EU.

On the other issue, it was noted that in spite of a ***large measure of convergence***, **substantial divergencies** remain concerning the rules on transfers to "third countries". First of all, there is again the matter of whether the **non-EU EEA States** should be treated as (or on a par with) the EU States. That aside, there are differences on how to treat "third countries" ***pending*** a finding of "**adequacy**" at the domestic or European level; and one country continues to allow free transfers of data to all State-Parties to Council of Europe Convention No. 108 even though that Convention does not, by itself, ensure "adequate" protection in all the States that are party to it.

The States also **differ** in respect of the detailed application of the ***derogations*** concerning transfer to countries without "adequate" protection. Some add additional, **stricter tests or requirements**, e.g. that the derogation concerning transfer to protect the ***vital interests*** of a data subject only apply if that person is incapable of giving consent to the transfer. One Member State ***excessively relaxes*** the rules concerning transfer of data to tax officials in third countries without protection, while two do <u>not</u> provide for the required derogation concerning transfers of data obtained from **public registers**.

matters to be further clarified or addressed

As already noted above, at 4, the question of whether - in view of the fact that the Directive has been added to the *acquis* of the EEA - the **non-EU EEA States** should be treated as EU Member States, or whether they should be treated as "third countries" (albeit "third countries" whose laws provide "adequate" or indeed "equivalent" protection) will be clarified by the Legal Service of the Commission.

Apart from this, the **freedom to transfer personal data to other EU** (or EEA) **Member States**, stipulated by the Directive, should be ***expressly re-stated in the laws of the Member States*** - but should at the same time be ***limited to matters within the scope of the Directive***. Transfers of personal data to the other Member States in connection with matters not within the scope of the Directive should be subject to the same approach as is adopted with regard to transfers to "third countries", i.e. they should be allowed if it has been formally determined that "adequate" (or indeed, given that data protection is included in the Charter, "equivalent") protection is ensured in respect of the processing of the data in the non-Community context in the other Member State, or if certain special derogations apply (which should be subject to appropriate safeguards).

The **rules on transfers** of data from the Member States to "third countries" will also have to be ***fully harmonised*** if evasion (made possible by the free zone for data transfers within the EU) is to be avoided.

- o – O – o -

14. transnational issues (ii) - cross-border transfers – detailed findings

14.1 EU\EEA and third countries

As already noted above, at 4, the Directive, in the context of transnational issues, distinguishes between "Member States" and other States; and it refers to those other States as "third countries" in the context of transborder data flows ("transfers" of data). The specific articles dealing with the latter question (Arts.25 and 26 of the Directive) are discussed below, at 14.2 and 14.3.

Before discussing them, it must be noted that, in that context (as in respect of "applicable law"), some of the EU Member States treat the non-EU Members of the **European Economic Area** (EEA), *Iceland*, *Liechtenstein* and *Norway* as EU Member States, while some treat them as "third countries". Oddly, however, the groups are not exactly in the same as in that other context.

Specifically, the non-EU EEA States are treated as EU Member States (as far as the issues of "applicable law" *and* transborder data transfers are concerned) in the laws of Denmark, Germany, Ireland, Sweden and the UK, and as (or on a par with) EU Member States in connection with transborder data flows in Finland (but, as we have noted, that country does not treat them as such in connection with the question of "applicable law").

Again, it must be noted that this question is not the same as the question (further discussed in this chapter) of whether the law in the non-EU EEA countries provide "**adequate protection**". By implementing the Directive, they clearly do. The problem is that (as noted below, at 14.3) "third countries" which provide an "adequate" level of data protection are still not treated in the Directive as "Member States".

As already mentioned above, at 4, the Commission has agreed to ask the Legal Service for clarification on what is the correct legal approach in this respect. Pending this advice, it must again suffice to note that the EU Member States which have implemented the Directive do not agree on this matter; that the laws accordingly show **divergencies** in this regard; and that this divergence will have to be addressed, on the basis of the Legal Service's advice, in the context of the revision of the Directive.

14.2 rules and procedures relating to intra-EU transfers

> "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with [data protection]." (Art. 1(2) of the Directive)

One of the main aims (indeed, perhaps, strictly speaking *the* main aim) of the Directive is to remove obstacles to the Single Market arising out of restrictions imposed by data protection laws on cross-border data transfers. The Directive seeks to ensure a high level of data protection so that those obstacles can be removed. Having done so, it can therefore lay down the principle of a "**free zone**" for data transfers throughout the European Community, as is done in the above-quoted provision. However, like all the other provisions in the Directive, this stipulation too of course only applies to matters within its own scope (that is, broadly

speaking, to matters within the scope of Community law). Indeed, a similar freedom cannot be stipulated in such an unconditional way for matters outside the scope of the Directive, because there is no guarantee that in such matters the same high level of protection is guaranteed. The two things hang together: freedom to transfer data where there is protection; no such freedom where this is not guaranteed.

This is not always - in fact, rarely - explicitly recognised in the laws of the Member States. Rather, most laws, by not laying down any specific restrictions on such transfers (while laying such restrictions down for transfers to non-EU States) **imply** that there are no restrictions on transfers to other EU Member States. If there is such implied freedom, this must, in these countries, moreover be assumed to apply to matters both ***within and without the scope of Community law***.

Only Austria has addressed these matters fully, expressly and properly. Its law stipulates ***expressly*** that "**the disclosure and transfer of [personal] data to recipients in EU Member States**" is not subject to ***any restrictions***, unless the transfer concern an **exchange of data between public authorities** in connection with ***matters outside the scope of Community law***. Greece and Portugal also stipulate the **freedom to transfer data within the EU *expressly*** - but these States do not limit this freedom to transfers in connection with activities within the scope of Community law.

The laws in all the other Member States, except for Germany, merely ***imply*** the freedom to transfer data to other EU Member States, by not subjecting such transfers to the restrictions which they *do* impose on transfer to non-EU (or non-EEA) States, but extend this implied freedom to matters both ***within and without the scope of Community law***. This applies to Belgium, Denmark, France,[112] Finland, Ireland,[113] Italy, Luxembourg, the Netherlands, Spain, Sweden and the UK. Of these, Denmark, Finland, Ireland,[114] Sweden and the UK extend this (implied) freedom to transfers to the non-EU EEA States (***Iceland***, ***Liechtenstein*** and ***Norway***), while the others (Belgium, France,[115] Italy, the Netherlands and Spain) limit it to the **EU States**.

The rules in the German law stand somewhat apart from the others, in that, on the one hand, they *do* **distinguish** between transfers ***within and without the scope of Community law***, but on the other hand do not unequivocally stipulate that transfers within the scope of Community law and within the EU (or the EEA: see below) are "**free**". Rather, the law in Germany gives effect to the principle of **free intra-EU** (or in terms of the Law, ***intra-EU\EEA***) **transfers** by stipulating (in a rather convoluted way) that - "**in accordance with the laws or agreements applicable to the transfer in question**" - transfers to ***recipients in EU\EEA countries*** which relate to **activities which are wholly or in part within the scope of Community Law** are ***subject to the ordinary German-legal rules on the processing and disclosure of personal data***. The proviso that these German rules apply "in accordance with the laws or agreements

---

112 Under the current (pre-implementation) law in France, the freedom to transfer data is extended to all the States-Party to the Council of Europe Convention on data protection (Convention No. 108), but this freedom is to be limited to the EU Member States under the proposed new (amended) law. Cf. the situation in Sweden, noted in the next section, section 14.3.

113 This is the case under the current (pre-implementation) law in Ireland, and is not to be changed under the proposed new (amended) law.

114 *Idem*.

115 Under the proposed new (amended) law.

applicable to the transfer in question" (*nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen*) presumably just means that if any **other legal rules** (or international agreements) apply to the transfer, they too ***must be adhered to***.[116]

The stipulation that transfers to recipients in other EU (or EEA) States must conform to the ordinary rules relating to the processing involved in the transfer is, as such, in accordance with the Directive. Thus, if the transfer involves a ***disclosure*** from one controller to a third party, that disclosure must be in accordance with the rules on disclosures in the "applicable" - i.e., in this case the German - law. However, it must be noted that in Germany these rules are often based on (slightly varying) and very abstractly formulated "**balance**" **tests**. It should be stressed that (from the point of view of the Directive), the fact that data are transferred to another EU country is a factor which should not be taken into account in applying such tests. Whether this will always be adhered to is perhaps somewhat doubtful, in particular in view of the fact that the law also lays down (separate but similar) "balance" tests with regard to transfers outside the scope of Community law, in the context of which the fact that the data are sent abroad ***will*** be a (major) factor to be taken into account. That however is a rather limited issue, which arises in that country only.

The more general problem in this regard is the absence of a distinction in the (implied) freedom to transfer personal data within the EU (or indeed, EEA) between matters within and without the scope of Community law. Just as with regard to the question of "applicable law", discussed in the previous section, the uncritical application of the basis rule in the Directive to matters not subject to the Directive can lead to **serious constitutional problems**, if the laws in the Member States concerned are seen as authorising unimpeded data transfers from Member States with (perhaps a high level of) constitutional protection to Member States which, in the area within which the transfer takes place, do not provide the same, or an "adequate" (or perhaps not even any) data protection. These issues are likely to arise, in particular, in sensitive "Third Pillar" contexts.[117]

---

[116] The proviso would not appear to refer to the possibility of another national law (of another EU\EEA State) applying to the transfer. However, it nevertheless of course remains the case that if the processing in the context of which the transfer takes place is subject, not to the German Law, but to the data protection law of another EU\EEA State, the lawfulness of the transfer too is to be judged by reference to that foreign law (only). However, it must also be recalled that the Gernan law does not quite follow the prescripts of the Directive in that regard: see above, at 4.2.

[117] Cf. the following note from Statewatch: "FORTRESS EUROPE - STAGE 2": EU BORDER POLICE PROPOSED On 7 May [2002] the European Commission produced a Communication entitled: "Towards integrated management of the external borders of the Member States of the EU". Its core proposals are (1) the creation of an "External borders practitioners common unit", (2) the introduction of a "security procedure" based on "direct links and exchanges" of "data and information between authorities concerned with security at external borders", (3) in the long term the creation of a European Corps of Border Guards with a "permanent headquarters staff structure charged with its operational command, the management of its personnel and equipment". Statewatch has prepared an analysis on the Communication which concludes "there is marginal reference to protection of asylum-seekers, **no mention at all of data protection or other human rights considerations**, and no suggested rules for the legal or political accountability or control of the common unit and the information system of the Border Corps. In fact the Commission explicitly suggests setting up the new information exchange system without any legal rules whatsoever governing its operation." See: http://www.statewatch.org/news/2002/may/06border.htm - Statewatch News Online, 20 May 2002 (emphasis added).

14.3 rules and procedures relating to transfers to non-EU\EEA countries

CHAPTER IV - TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25 Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection,

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26 Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation" are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

The laws of almost all the Member States - Austria, Belgium, Denmark, France,[118] Finland, Greece, Ireland,[119] Italy, the Netherlands, Portugal, Spain, Sweden and the UK - clearly contain the **in-principle prohibition of transfer to "third countries" without "adequate" data protection**, set out in Art. 25(1) of the Directive, quoted above. The Austrian law does so by reference to the permit-system established under that law, but the principle is still clear. In determining such "adequacy" the above countries also take the same matters 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; the Irish law referring to "codes of conduct or other [sectoral] rules which are ***enforceable*** in that country or territory"; and the proposed new French law simply to "***rules in force***" in the other country.

[118] Under the proposed new (amended) law: as noted in footnote 105, above, and as further discussed in the text, the current (pre-implementation) law still focusses on transfers to other States-Party to the Council of Europe Convention on data protection.

[119] The relevant rules, based on the Directive, have already been incorporated into the current Irish data protection law by virtue of regulations introduced in 2001; they are merely re-stated (in identical terms) in the proposed new (amended) data protection law. In this section, I will therefore refer quite simply to "the Irish law" or "the law in Ireland", rather than to "the current (pre-implementation" law, or "the proposed new (amended) law", as I have done elsewhere.

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. This could have significant repercussions, but will perhaps not be applied strictly (the law not yet having come into force, there is of course still no practice).

The German law is somewhat ambiguous in this respect, by stating the in-principe 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 focusses 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.

Also, as discussed above, at 14.1, Denmark, Finland, Ireland, Germany, Sweden and the UK do not regard the **non-EU EEA States** (***Iceland***, ***Liechtenstein*** and ***Norway***) as "third countries" in this respect, and they therefore do not apply the in-principle prohibition to these countries, whereas the other Member States - Austria, Belgium, France, Greece, Italy, Luxembourg, the Netherlands and Spain - *do* regard these three countries as "third countries".

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", as discussed below) ***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", transfer of personal data to that country are ***subject to the in-principle prohibition***. That is: they may only take place on the basis of one of the specified derogations. 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 themselves believe that the laws or regulations in the country in question (or indeed in the sector in the country in question) are "adequate". 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). While for many non-EU\EEA countries it will perhaps be obvious that they do not provide "adequate" protection, there will be others for which this is less clear, and there can be further differences of views if one were to look at specific sectors. The different approaches to this question pending formal findings therefore result in **substantial divergences** between the Member States. In this regard, the remark by the French data protection authority, that it "has never encountered a situation in which a transborder flow of [personal] data violated the provisions of the Directive" would appear to be, if not naive then indicative of a desire to "see no evil, hear no evil, speak no evil."

The issue has been specifically addressed - in remarks which are generally critical of the Directive's detailed rules - by the UK data protection authority (the Information Commissioner), who said:

> "The principle that data controllers should not transfer personal data outside the EU unless the data will be adequately protected is sound. However **the terms of Articles 25 and 26 are over-prescriptive and place undue emphasis on centralised decision making**. The general position with data protection law, at least in the UK, is that it is for data controllers to ensure they comply with the law. Their activities are not subject to prior approval but if they are found not to be complying they may face a sanction. There is no reason to depart from this approach with international transfers. The idea of a list of third countries where because of their law there can be a presumption of adequacy undoubtedly assists data controllers but outside this it should be for data controllers to make their own decisions and arrangements for adequacy. They may choose to use contractual solutions but there should be no requirement for these or other arrangements to be approved in advance by either the Commission or by Member States. The UK law has been written and is interpreted in a way that favours this approach but the scope for doing so is unnecessarily and unhelpfully limited by the Directive."

It should also be noted that the law in Sweden allows transfers of personal data to ***all the States which are Party to Council of Europe Convention No. 108*** (provided the data are not further transferred to countries not party to that Convention), although the Working Party has found that in several respects the Convention does not (fully) ensure such "adequacy". This is not so much because Sweden disagrees with that finding but because Sweden accepted the duty to allow transfers to such States under that treaty long before it even joined the EU. As noted earlier, France, by contrast, has expressly (and deliberately) changed its earlier practice on these lines, and under its proposed new (amended) law will limit the freedom to transfer data to EU Member States only.

It may be added that the laws in Austria, Finland, Ireland, the Netherlands, Spain, Sweden, Portugal and the UK, and the proposed new law in France, all expressly ensure that if and when the Commission does make a "finding of adequacy" under Art. 25(6) of the Directive (as it has done in respect of ***Hungary*** and ***Switzerland*** and as concerns companies adhering to the "***Safe Harbor***" principles in the ***USA***), such findings are given effect domestically, but that this is not explicitly provided for in the laws in Belgium, Germany, Greece, Italy and Luxembourg (although this of course does not mean that such findings cannot be given effect). The Luxembourg law does however require 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, allowing for the implementation of (various kinds of) EC decisions on the implementation of the Directive has not been used.

As far as the **derogations** listed in Art. 26 of the Directive are concerned, the Member States have ***generally*** **closely followed the text** of the provisions in that Article. However, there are also matters in which the laws **differ** from the Directive (and from each other).

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**" (if one assumes that the legal instruments referred to all serve such interests) - 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 long as the wider derogation is only applied to matters outside the scope of Community law, e.g. to "Third Pillar" matters - and hence outside the scope of the Directive – this does not involve a breach of the Directive. However, the different standard underlines the difficulties of applying a different regime to matters within and without the scope of the Directive, as discussed above, at 3.3.

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***"; and that law also (as in respect of processing of "sensitive data", discussed above, at 7.2) 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***". By contrast, the Luxembourg law (which as such follows the text of derogations set out in the Directive closely) requires generally that "**consent**" be "***unambiguous***" and "***explicit***" (see above, at 2.8 and 6.2). The proposed new (amended) French law also stipulates that "**consent**" for transfers to countries without "adeqate" protection must be "***expressed***" - which in the context of that country means that it must be ***in writing*** (although it may be possible to "express" such consent on the **Internet** by means of a "***double click***", as discussed above, at 7.2 with regard to the similar requirement concerning "sensitive data".

The Austrian law is ***strict*** as concerns transfers in connection with a **contract**, in that it says that data may only be transferred if they are ***essential***. 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 "**claims before *foreign legal fora***" (which is more limited than in the Directive) 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. On the other hand, the law **adds** derogations in respect transfers of information what has been "***lawfully* published**", "**indirectly identifiable data**" (i.e. encoded or pseudonymised data), transfers specifically envisaged in (read: authorised by) an **Austrian law**, and relating to "Third Pillar" matters such as **national security**, **defence**, the **prosecution of offences**, etc.

The laws in Greece and Italy also add to the derogation concerning transfer of personal data to protect the **vital interests of the data subject** the proviso that this derogation only applies if the data subject is (legally\mentally or physically) ***incapable*** of giving his or her consent to the transfer, while the proposed new law in France again refers to processing (or her, to a tranfer) which is necessary "***to safeguard human life***".. The law in Greece limits the derogation to protect **important public interests** in a manner similar to the Austrian law, to cases in which there is an ***exceptional need***, while the proposed new law in France, by contrast, merely refers to transfers which are "necessary" "***to safeguard the public interest***" - although in practice, this could be restrictively applied.

The law in Austria also does not contain a special derogation with regard to data obtained from **public registers**, envisaged in the Directive. The general data protection law in Sweden

itself also does not contain such a derogation with regard to data obtained from a **public register** - however, in that case the legislative approach (discussed above, at 3.4) according to which special issues are determined in special laws rather than in the general ("omnibus") data protection law means that 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. The Italian law contains a special derogation allowing for transfers of data by **journalists**, provided they act in accordance with the special ***code of conduct for journalists***, adopted under the law, and the French law (both current and proposed) also makes an exception for **journalists**, subject to compliance with the relevant legal and self-regulatory rules (as noted above, at 10.1).

The law in Spain (like the proposed new law in France) 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." That law also contains some further derogations concerning "Third Pillar" matters and a special derogation concerning processing "related to **money transfers**" (provided the data transfer is in accordance with special legislation on such transfers). These derogations may appear more lax than envisaged in the Directive. However, in the light of the Constitutional Court ruling referred to in section 3.4, above, they must be interpreted strictly, and they are interpreted strictly by the Spanish Data Protection Authority. Transborder transfers of data must therefore - like all other processing - be ***necessary for specific, strictly defined purposes laid down in a formal statute adopted by Parliament***. In fact, even before the ruling, the Authority required, as a basic minimum, that the transfer was based on a legal regulation of the appropriate level allowing the transfer. Applied in accordance with the Constitutional Court ruling, the derogations in the Spanish law thus fall in line with the Directive.

The UK law allows the Lord Chancellor to ***specify*** when transfers must be considered to be necessary on "**important public interest grounds**" - which means that the question of their "necessity" can not be further reviewed.

Finally, as concerns the derogations provided for in Art. 26(1) of the Directive, the laws in both Denmark and Germany, and the "***Instruction***" issued in Spain (discussed below) add explicity that cross-border transfers remain **subject to the normal legal rules in the domestic law**. For instance, if the transfer involves a ***disclosure to a third party***, that disclosure must be lawful under the Danish or German law (or possible another "applicable" law); the usual (and any special) ***informing-*** or ***notification-requirements*** must be complied with; etc. As such this is uncontroversial: it will apply in all the other States as well. However, a *caveat* must perhaps again be entered in respect of Germany, in that the law in that country often allows certain matters (such as disclosures) on the basis of rather vaguely-phrased "**balance**" tests. There is a risk that in applying such tests, the fact that the processing involves a cross-border transfer will be taken into account, and the tests applied in ways which restrict transfers further than envisaged under the Directive. The German law also lays down certain ***additional restrictions*** with regard to **purpose-limitation** in connection with cross-border data transfers.

All but one of the laws of the Member States also specifically provide for the possibility of allowing transfers on the basis of **contractual clauses**. The only country in which this is not

expressly done is Greece. The law in the Netherlands suggests that such clauses are to be drafted by the Dutch ***authorities*** rather than by controllers, as is suggested in the Directive - but in practice this is of course very much a matter for consultation between authorities and controllers, in that country as much as elsewhere. Most of the Member States have not taken major steps in this regard at the domestic level, because of the efforts being made in various international fora, and in particular by the Commision. An exception is Spain, in which the Data Protection Authority has issued a detailed "***Instruction***" on transborder data transfers, which includes a list of matters to be included in such contracts. An extract from the "***Instruction***" containing this list is attached to this section for information. In France, the data protection authority has been asked to review contract clauses drafted by companies on many occasions (some 200 to date, covering about 50 draft contracts).

Overall, there are therefore again - in spite of a ***large measure of convergence*** - **also divergencies**. First of all, there is again the matter of whether the **non-EU EEA States** should be treated as (or on a par with) the EU States. That aside, there are differences on how to treat "third countries" ***pending*** a finding of "**adequacy**" at the domestic or European level, and one country (Sweden) allows transfers to all State-Parties to Council of Europe Convention No. 108. The States also **differ** in respect of the detailed application of the ***derogations*** concerning transfer to countries without "adequate" protection. Some add additional, **stricter tests or requirements**, e.g. that the derogation concerning transfer to protect the ***vital interests*** of a data subject only apply if that person is incapable of giving consent to the transfer. Spain ***excessively relaxes*** the rules concerning transfer of data to tax officials in third countries without protection; Ireland stretches the concept of a data subject's (or someone else's) "***vital interests***" beyond what is elsewhere considered to be caught by those words; and Austria does not provide for the required derogation concerning transfers of data obtained from **public registers**.

ATTACHED: Extract from the "Instruction" issued by the Spanish Data Protection Authority on the rules governing international data movements.

- o – O – o -

ATTACHMENT TO SECTION 14.3 (transfers to non-EU\EEA countries):

Extract from the Spanish Data Protection Authority's Instruction on the rules governing international data movements (Instruction 1/2000 of 1.12.2000)

"[The authorisation provided for in Art. 33(1) of the Spanish Data Protection Law] shall be granted if the controller produces a written contract between the transmitter and the recipient which provides the necessary guarantees to protect the data subjects' privacy, their fundament rights and freedoms and the exercise of their corresponding rights. The contract in question must provide the following, as a minimum:

a) the identity of the transmitter and the recipient of data;

b) the purpose of the international transfer and the data to be transferred;

c) an undertaking by the transmitter that the collection and processing of the data on Spanish territory comply fully with the rules contained in [the Law] and that the file on which the data for transfer are recorded is entered on the General Data Protection Register;

d) an undertaking by the recipient that it will process these exclusively for the purpose given as the reason for the transfer and in accordance with the data protection standards of Spanish law and an undertaking not to communicate the data to any third party without having obtained the consent of the data subjects;

e) an undertaking that the recipient will adopt the security measures required by the laws on personal data protection in force in Spain;

f) an undertaking that the transmitter and recipient shall be jointly and severally liable vis-à-vis private individuals, the Data Protection Authority and the Spanish legal authorities for any breach of the contract by the recipient which breaches [the Law] or causes injury to the data subjects;

g) an undertaking that any data subject injured as a result of the processing by the recipient shall be compensated in accordance with the liability system referred to in the previous paragraph;

h) a guarantee that the injured party may exercise his rights of access, correction, cancellation or opposition vis-à-vis the data transmitter and recipient of the data. It must also be stated that a data subject whose rights are infringed may ask the Data Protection Authority to intervene on the terms provided in [the Law];

i) an undertaking from the data recipient to grant access to the establishment where these are being processed, to documentation, hardware and software to representatives of the Data Protection Authority or an independent entity appointed by the former when required for the purposes of verifying compliance with the obligations arising from the contract;

j) an undertaking that, once the contractual relation has ended, personal data must be destroyed or returned to the transmitter along with any medium or document in which any personal data on the subject is contained;

k) an undertaking that data subjects may require compliance with the provisions of the contract in all matters in which it is to their benefit."

15. codes of conduct *et al.*

introduction

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

Self-regulatory codes of conduct have been seen as a useful means to clarify the application of data protection law in a particular sector for some time, and the above provision in the Directive confirms that this is seen as a possibly effective instrument in this regard. In particular, **self-regulatory codes can be used as an alternative to sectoral regulation**: in theory, the drafting of codes should be a simpler, more flexible means to achieve the same end, the laying down of sector-specific rules applying the more general data protection rules. In practice, self-regulation and State-imposed sectoral regulation are not as different as one might expect: self-regulation increasingly takes place in a legal framework which allows for, or indeed requires, the assessment and\or approval of *soi-disant* "voluntary" codes, while State regulation may involve the drawing up of rules in consultation with (or even by) sectoral organisations. The stipulations in the Directive confirm this trend towards what one may call ***quasi-self-regulation*** (whereby it may be noted that the paragraph concerning Community Codes clearly envisages the "approval" of such codes, while the paragraphs concerning national codes refer more vaguely to the obtaining of an "opinion").

summary of findings

The laws in all the Member States (or in one case, a Decree issued under the law) now include provisions on the drafting of **self-regulatory codes of conduct** (with some differences in terminology, e.g. some refer to ***deontological codes*** and one to ***sectoral agreements***). In most, the laws refer to the "**checking**" or "**assessing**" of the compatability of the code with the law and\or to the issuing of an "**opinion**" on that conformity - thus retaining the ambiguity with regard to the status of such codes, noted in the Introduction to this section. However, the law in Luxembourg refers to the "**approval**" of codes by the national authority (and mentions the "approval" of of Community-wide codes by the Working Party established under the Directive in the same breath). The law in one Member State (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. The proposed new law in France expressly stipulates that, when the amended version of the law comes into force, the data protection authority must re-examine the codes on which it has previously given a positive "opinion", in the light of the new provisions.

The laws in several Member States show features which reflect the trend towards ***quasi-self-regulation*** also noted in the Introduction. 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** (which 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 Ireland, the proposed new (amended) law, if adopted in its current form, will build on the provisions concerning codes of conduct in the current law (which however have never been used), but also provides for the issuing of codes of practice by the data protection authority. Indeed, such "imposed" codes could (like codes drafted by industry) be further approved by the Irish legislator (the *Oireachtas*), which would give them **binding legal effect**. The Commissioner had the following to say on the matter in his latest (2001) Annual Report:

> "I am disappointed that no proposal for a statutory Code of Practice has been brought forward by any representative association in Ireland. I anticipate, however, that the forthcoming implementation of amended data protection legislation will provide a new impetus in this area ... It is also significant that [the proposed new (amended) law will allow me] to bring forward proposals of my

> own for sectoral codes of practice. While it is my undoubted preference for such codes to emanate from the representative associations themselves, I will certainly consider myself free to have full recourse to this new power wherever I consider that the best interests of data subjects so require. Naturally, any actions in this area would be on the basis of full consultation with all interests affected, including both representative bodies and the public more generally."

He therefore went on to give detailed guidance, in that report, on the matters that should be addressed in particular in acceptable codes of conduct:

- what types of personal data are covered;
- for what purposes are these data processed;
- how are the personal data obtained;[120]
- how can the personal data be processed;
- to whom will the personal data be disclosed; and
- for how long will the personal data be retained?

In Greece, the authority generally prefers to rely on the issuing of its own sectoral rules (rather than on 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) - but elsewhere (e.g. in the UK) the possibility of issuing State-imposed sectoral rules is regarded more as a "stick behind the door", to be used only if a sector does not itself put forward adequate rules.

Codes do get adopted and (positively) "assessed" in many countries - but the process is often tortuous and the number of codes issued in this way is only limited. In France, for instance, only some six codes have been adopted in 25 years - and five of concern the related matters of direct marketing, distance selling, lifestyle databases, call centres, and *e*-mailing. As I noted in an earlier study already referred to,[121] there is a certain tension between the views taken of codes by industry and regulators. The former sometimes feel that the latter are too rigorous in their initial assessments of draft codes submitted for an "opinion", while the latter sometimes feel that the former are trying to use codes as a means to evade certain strict rules in the law. The process for obtaining an "opinion" or assessment is consequently often long (as is also the case, it may be noted, with regard to the approval of Community Codes).

---

120 The Commissioner discusses under this heading the question of what kind of consent may be required for different purposes, as noted above, at 6.2 and (with regard to direct marketing) at 9.3.

121 Study into *4on compliance with the data protection laws and principles in the Member States of the European Union* (above, footnote 104).

matters to be further clarified or addressed

In view of the principle of subsidiarity, there is no need to prescribe a particular procedure for the adoption of codes of conduct, or to prescribe a particular status for such codes. However, it might be advisable to stress that the process for adopting draft codes should not be too cumbersome (whereby it could be added that the operation of a code in practice can be, and should be, kept under review). For the purpose of the Internal Market, the adoption of Community codes is of course more important - but that is not a matter to be addressed in this comparative summary of national laws.

o – O – o -

16. the supervisory authorities

introduction

The Directive requires the Member States to assign the task of monitoring the application of (i.e. compliance with) their national laws to certain special **public authorities**, referred to in the Directive as "***supervisory authorities***" but also often called "***data protection authorities***" or "***-commissioners***". The Directive stipulates that these authorities must "***act with complete independence***", and must be given certain ***investigative***- and ***enforcement powers***, the power to either themselves engage in ***legal proceedings*** or to bring relevant matters to the attention of the ***judicial authorities***, a separate power to "***hear claims***" (complaints) from data subjects or associations representing data subjects, and certain further duties including the publication of an ***annual report*** and ***co-operation with other data protection authorities*** and ***with the Commission***. It is important to note that these stipulations are not so much a prescription of an ideal authority, conceived in the abstract, as a reflection of the status, tasks and powers of the authorities in existence before the Directive was drafted, with a certain emphasis on what were thought to be essential features of effective authorities, but also with enough flexibility built in to allow Member States to choose their own model.

The study examined the actual **status**, **tasks**, **functions** and **powers** of the national authorities in the light of the Directive's general provision. In this, it built on an earlier study by the consultant for the Commission, which covered these matters under the previous laws.

summary of findings

The study found that the laws in the Member States all grant their data protection authority or authorities formal ***independence*** in the exercise of their functions. However, they are clearly not **judicial bodies** and usually closely linked to the **Ministry of Justice**. Perhaps the best way to describe them is as "***independent administrative agencies***".

They are given **a wide range of tasks**, including ***informing- and publicity functions***, ***administrative functions***, ***regulatory functions***, ***quasi-legislative functions***, ***quasi-judicial functions***, and ***investigative and enforcement functions***. In the latter context, they are given **astonishingly wide and strong powers of search and entry**, often exercisable without a judicial warrant; and also often powers to **order** that data be "***blocked***" or processing ***stopped***, subject to the imposition of **administrative fines**.

Furthermore, implementation of the Directive does not appear to have changed the **generally advisory and concilliatory approach** of the national data protection authorities (noted in the earlier study) which - while helpful in many ways - can also lead to the impression that **enforcement** is rather "***soft***" and perhaps even ***negotiable***; and **data subjects** are still not always kept fully ***informed*** of the outcome of complaints (let alone given a chance to influence this outcome).

matters to be further clarified

As a matter of principle, in States under the Rule of Law, the very existence of the above-mentioned kinds of **almost discretionary powers** in the hands of **non-judicial bodies** must raise questions. At the very least, the exercise of such powers should be subject to ***judicial overview*** and indeed, in appropriate cases, to ***prior judicial authorisation*** (such as the issuing of a search warrant). There should furthermore be safeguards in place to ensure that the law is applied both **equally** (with all controllers being treated alike) and in such a way as to fully uphold **data subject rights**. This means that ***full information on all enforcement actions*** of the authorities should be publicly available; and that ***data subjects are always fully informed*** of the outcome of any complaints, and involved in the process. In cases of disagreement (either between controllers and the authorities or when data subjects are not satisfied with the result of an authority's actions) ***effective*** and ***effectively available*** (i.e. cheap) ***judicial remedies*** should be available to all interested parties.

These matters are of particular importance in connection with the exercise of other fundamental rights, such as the right to **freedom of expression** (including the right to seek, receive and impart information regardless of frontiers) and **freedom of information** (in the sense of a right of access to official documents). Indeed, one might question whether data protection authorities (as currently constituted) are the appropriate bodies to adjudicate on, and\or impose restrictions on the ***press*** and others exercising their right to freedom of expression (such as ***human rights organisations***).

- o – O – o -

16. the supervisory authorities – detailed findings

Article 28
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political Institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

The provision in the Directive, quoted above, is not so much a prescription of an ideal authority, conceived in the abstract, as a reflection of the status, tasks and powers of the authorities in existence before the Directive was drafted, with a certain emphasis on what were thought to be essential features of effective authorities, but also with enough flexibility built in to allow Member States to choose their own model.

In practice, data protection authorities everywhere are rather strange "beasts", given an impossible range of (some would say, incompatible) tasks, enormous powers - and too few resources to be truly effective. This is not the place to discuss or compare and contrast purely technical matters (appointment procedures, terms of office, etc.): differences in such matters do not affect the Internal Market. Rather, I will here reflect briefly and in general terms on the **status**, **tasks** and **powers** of the authorities in the Member State, with reference to an earlier study I carried out for the Commission, already referred to, in particular in connection with notification (above, at 12).[122]

The main point about their **status** is the question of their ***independence***. The Directive says that they 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. The laws in most countries do indeed stress that the authority "shall be an independent authority"; "shall not be subject to any directions in the exercise of its functions"; etc. Many are appointed in special procedures, often involving **Parliament** - although some are appointed by the **Government** (Ireland, Luxembourg, UK)[123] or indeed by the **Minister of Justice** (Denmark, Netherlands). In France, the authority is made up of representatives of the two Chambers of Parliament and of members chosen by the Social and Economic Council, the *Conseil d'Etat* and the Court of Cassation, the Court of Auditors, and the Government. In Portugal, most members are appointed by Parliament, but some by others: a judges is appointed by the Superior Judicial Council, a procurator by the Procuracy, and two members are appointed by the Government.

In Germany, there is a federal data protection authority, responsible 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*; while processing by private-sector controllers (although subject to unified substantive rules in the federal data protection law) is supervised by still further, often separate authorities. The federal and *Landes*-data protection authorities are (like the national data protection authorities in the other Member States) usually appointed by their own parliaments - but the authorities charged with supervising the private sector are, in many *Länder*, (part of) a local government or ministry - although in several of the *Laender* the law has been changed to make the *Landes*-data protection authority the supervisory authority in respect of private-sector processing too.[124] Ministries are, by their nature, not "***independent***" and it is therefore surprising that - in spite of a requirement of independence in Art. 28(1) of the Directive - all but one of the *Länder* which have adopted new data protection laws in order to comply with

---

122 Study into *Existing case-law on compliance with the data protection laws and principles in the Member States of the European Union*, see footnote 104, above.

123 Formally, the Luxembourg authority is appointed by the Grand-Duke, on the basis of a proposal from the Government; and the UK data protection authority (the Information Commissioner) is appointed by the Queen, acting on the advice of the Government.

124 The State Data Protection Commissioner has been made the "supervisory authority" for the private sector in Berlin, Bremen, Hamburg, Lower Saxony and Schleswig-Holstein.

the Directive have nevertheless left external supervision over processing by private-sector controllers in the hands of their Interior Ministries.[125]

The members' appointment is everywhere for a ***specified period*** (somewhere between four and six years). However, they are also often **close to Government departments**, usually the ***Ministry of Justice***. Indeed, in several countries the law specifically links the Authority to that Ministry (while also stressing their independence). In many countries the Authority is furthermore either composed of representatives from a range of backgrounds (Parliament, industry, consumers, IT specialists, often the judiciary) or adviced by a broad-based Council. These Authorities are clearly not **judicial bodies**. Perhaps the best way to describe them is as "***independent administrative agencies***".

The Authorities in the Member States are given **a wide range of strikingly similar tasks**, including:

- **informing- and publicity functions**, such as providing the public with ***information on subsidiary regulations*** issued under the Law; providing data subjects with ***general information*** on their ***rights***, and issuing an ***annual report***;

- **administrative functions**, in particular in respect of ***notification*** (registration of particulars of processing operations and their inclusion in the relevant register);

- **regulatory functions**, such as the duty to issue ***authorisations*** under the Law (e.g., in respect of transborder data flows);

- **quasi-legislative functions**, such as the issuing of ***instructions*** on how to bring specific kinds of processing operations into line with the domestic law, or how to apply the law in a particular context, including involvement in the drafting and assessing of **codes of conduct**;

- **quasi-judicial functions**, including in particular the "***consideration***" of – and sometimes ***adjudication*** on - ***applications and complaints from data subjects***"; and

- **investigative and enforcement functions**.

---

[125] Brandenburg, Baden-Württemberg, Bavaria, Hessen and North-Rhineland-Westphalia. The exception is Schleswig-Holstein. One could argue that the "supervisory authorities" *cum* Ministries, in spite of being part of the (State) Government, nevertheless "act with complete independence in exercising the [data protection supervision] functions entrusted to them" (which is the wording used in the Directive). However, as Dammann and Simitis rightly point out, that wording in the Directive was intended to underline that the authorities not only had to ***be*** independent but **also** had to ***act*** independently: EG – Datenschutzrichtlinie – Kommentar, Comment on Art. 28 of the Directive, margin note 5. One could also argue that "independence" here means independence from the parties involved, i.e., in respect of processing by the private sector, of the controller and the data subjects. However, it is (in my opinion) disingenious to suggest that the Government and the public administration do not have an interest in the regulation of private-sector processing. Interior Ministries are also closely associated with (and legitimately influenced by) politics. To that extent, it is difficult to see how such a Government Ministry could truly "act independently"; at the very least, the *appearance* of partiality would be unavoidable. Cf. also the case-law on the terms "impartiality" and "independence" by the European Court of Human Rights.

Having already dealt with notification and (prior) authorisations (and "checks") in section 12, above, and having alluded throughout this study to various instructions and subsidiary rules, I will limit my comments here to the first and the last two of the above-mentioned matters.

As far as the **informing- and publicity functions** of the authorities are concerned, I may recall that they play an important role in the giving of advice on data protection matters, first and foremost to the legislative and executive authorities, but also to data users and groups of data users (sectors). They are, moreover, all required to issue an annual (or bi-annual) report on their activities. These functions are reflected in the Directive (see, in particular, Art. 28, paras. (2) and (5) of the Directive).

The advice thus provided - in the form of reports, studies, opinions or deliberations on proposed laws or regulations, or on general issues of importance in the field of data protection - is undoubtedly of crucial importance to the development of the law and practice in the Member States. Governments and legislators often follow the authorities' advice; at the very least, their opinions ensure that the issues concerned are properly aired and debated. The Annual Reports of the data protection authorities are furthermore mines of information and of considered, authoritative opinions on all matters relevant to the protection of fundamental rights of individuals in relation to the processing of personal data.

The issuing of such advice or reports is not "regulatory" as such, but this aspect of the authorities' work is nevertheless closely linked to their regulatory and enforcement activities: the general reports identify areas of particular concern, and therefore likely to be the subject of investigation and control, while "advice" on certain matters will often entail interpretations of the law - which will be carried over into supervision and enforcement. In several national systems, the providing of "opinions" furthermore formally or effectively becomes a part of enforcement. Thus, in France, the issuing of "favourable opinions" on the required regulations for proposed public-sector processing operations has in practice become a pre-condition: although in theory a "negative opinion" can be overruled by reference to the *Conseil d'État*, this avenue has never been used in practice. In the Netherlands, a positive opinion, by the data protection authority, is required before a (supposedly self-regulatory) sectoral code of conduct can play its intended role in the data protection compliance system. A further crucial link between reporting and enforcement is created by the fact that the "case-law" of the national data protection authorities is primarily to be found in the authorities' annual reports.

However, the overall reporting by many national authorities is not easily accessible, structured or comprehensive. Thus, many annual reports only contain selected deliberations, opinions or decisions. Many issues are furthermore reported on within the context in which they arose - e.g., national security, policing, the press, etc. etc. – although of course a ruling or opinion given in one context can have wider implications in other contexts, or generally (e.g. when it involves the interpretation of a particular term in the law). Comprehensive and structured information on all the views, opinions and rulings of the national authorities is not easy to come by. In countries in which the national data protection law is the subject of extensive and detailed commentaries (e.g., Germany), this may to some extent be remedied by academic gloss - although such commentaries do sometimes mix authoritative rulings and academic opinion in a somewhat confusing way.

I may therefore perhaps repeat the conclusion I reached in my previous study: that more systematic, structured and mutually compatible systems of reporting would facilitate the harmonised (or at least compatible) application of the Directive in the Member States, and would provide better insight into the operation of the national laws and the Directive generally.

All the 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 ("full") 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, e.g. because of the importance of the processing in the sector concerned, or the sensitivity of the data or of the operations in question, or because of the level of complaints received about the sector.

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 authorities have started to carry out extremely detailed "**privacy audits**" of selected data users, again to ensure that all relevant matters are closely examined. Under the proposed new (amended) law in Ireland, the data protection authority will also be vested with a strong power to carry out **audits** - also without the agreement of the controller. In the UK, on the other hand, the data protection authority cannot carry out such **audits** without a controller's agreement - which is something which the authority would like to see changed.

In most countries (but notably not in the UK), 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. Specifically, in Germany, the authorities have been given much wider, and stronger, powers as a direct result of the implementation of the Directive (although it is perhaps too early to asses the effectiveness of these new powers). If they believe that matters are amiss, the Authorities may usually **order remedial action** - usually subject to an appeal to a ***court*** or a special ***tribunal***, although often data can be "**blocked**" by the Authority, or processing **stopped** pending such an appeal in urgent cases in which there is a serious threat to the rights and interests of individuals. In addition, in many countries, the Authorities can impose **administrative fines**. However, such formal actions are, *in practice*, used only as a **very last resort**.

In reality, the data protection authorities in all the Member States see themselves much more as ***advisers, facilitators and concilliators*** than as policemen: referees rather than Rambos. As the UK data protection authority once put it:

> "Powers of enforcement are vital but our approach is to seek to anticipate complaints by providing adequate advice, or where they arise to proceed by agreement and negotiation only taking formal enforcement action where action to achieve compliance cannot be agreed." (Annual Report 1996, p. 32)

In all the Member States, the vast majority of investigations are resolved in this way: even if fairly blatant violations of the law are found (such as non-registration of processing

operations), the authority will usually first only issue a "reminder", "warning" or "advice" - and it will not resort to more formal measures unless these "softer" measures are ignored (or disputed: in some cases, data users who are advised that a certain practice violates the law may wish to challenge that advice, e.g. when matters of law or principle - or, more often, money - are at stake; in such cases, the users may therefore effectively invite formal enforcement action, in order to test the views of the authority in the courts).

Such general investigations are extremely useful and important as a means of clarifying the application of the law in a particular, practical context; reports on (selected) investigations therefore rightly take up a large part of the annual reports of the national authorities. They are, however, extremely costly in terms of time and resources, and can by their very nature only be very selectively used.

The authorities also pride themselves on the *effectiveness* of their "concilliatory" approach, pointing out that they have to resort to "hard" enforcement measures in only a very limited number of cases. However, the fact that such measures are rarely used does not of course prove that the outcome of the "concilliation" has led to strict adherence to the legal requirements. In particular, that approach can become rather **subjective and discretionary** (not to say negotiable or arbitrary): the outcome can seem to be a matter of ***compromise*** reached between the authority and the data user, rather than a solution imposed on the basis of a purely legal ruling.

It would appear (and indeed common sense would agree) that if the authority has a "stick behind the door", it can - and will be - more forceful in such attempts at "concilliation". Thus, the CNIL in France has, on occasion, imposed strict conditions on processing operations which could not lawfully commence until a "receipt" or "opinion" had been issued by the authority. Elsewhere, too, the threat of formal action (e.g. the issuing of a "preliminary" enforcement notice in the UK), or even less informal threats have been used effectively to "persuade" a data user to accept the solution "proposed" by the authority.

On the other hand, on other occasions "success" (in the sense of reaching a compromise without having to resort to "hard" enforcement) has been bought at too high a price, with "solutions" being accepted by the authorities which did not adequately protect data subjects. The case of the *renseignements généraux* in France (in which a regulation for this secret police service was first "approved" by the CNIL but then had to be withdrawn under public pressure) is a case in point. For some critics, the fact that in many cases the outcome of what are in effect negotiations between data users and data authorities are not reported in detail underlines the fear that perhaps **unduly lenient** "**deals**" are struck behind closed doors. Finally, the "concilliatory" approach by the data protection authorities can reinforce the idea on the part of many data users that ***data protection is "soft" law***.

Action taken by the data protection authorities on the basis of **complaints from individual data subjects** follows the ***same pattern***: the authority gets in touch with the data user concerned, "advices" and acts as a concilliator, and tries to reach an amicable solution to the dispute. In many cases, the issues are straight-forward and easily resolved on the basis of clear legal principles. For instance, a data user refusing to grant a data subject access to his or her data may need only to be "reminded" by the authority of his duty to allow such access. Other cases however are more complex, and in those the authority tries to reach a compromise acceptable to both the data user and the data subject. Again, this approach is almost always

"succesful", in the sense that the authority does not need to use formal enforcement measures: the authorities in the Member States only resort to "hard" enforcement measures in a minute proportion (a few per cents) of complaints. Again, however, it is difficult to assess the true effectiveness of this approach: the annual reports by the national authorities do not generally provide a breakdown between (say) the number of complaints in which the authority found that there had been a breach of the law (and in which the law was enforced in a straight-forward way), and the number in which the authority negotiated a compromise; and they also do not give an indication of the level of satisfaction with the process on the part of the complainants.

Overall, it is clear that investigations by the national authorities into general issues or specific complaints are **meticulous, in-depth and detailed** - but require large resources which can only ever be made available on a selective basis. The outcome can, at times, appear to be somewhat "soft" and seemingly negotiable - but this can be remedied in substance by ensuring that the authority, if necessary, can resort to "harder" measures, and on appearance by wider reporting of the "compromises" reached.

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. Thus, in the UK, the data protection authority can refuse to register a prospective data user if the proposed processing operation appears to contravene data protection principles, or she can issue a de-registration notice or other enforcement notices demanding compliance. In France, the CNIL can similarly refuse to issue a "receipt" in respect of a registered operation, or order changes to a processing operation on the basis of the findings of an investigation. Similar powers are granted elsewhere - except, that is, in Germany, where the data protection authorities can, ultimately, only "warn" (*beanstanden*) data users in respect of processing they regard to contravene the law.

It will be clear from the above that the data protection authorities, in all the Member States, in practice only ***extremely rarely*** seek to apply such **formal sanctions** to data users violating the law: most matters of contention (including manifest breaches of the law) are dealt with less formally, through ***discussion and negotiation***.

Criminal prosecutions are similarly ***extremely rare***: in the UK, the annual level of prosecutions is about 55, of which about 30 are for the (rather straight-forward and easy-to-prove) offence of non-registration. This compares with estimates of several hundred thousand data users who have in fact failed to register and who are therefore, in principle, liable for prosecution. In France, the CNIL is even more reluctant to use its powers to "denounce" data users who break the penal provisions in the data protection law: there have only been 18 "denunciations" since the adoption of the law in 1978 (including, last year, the first one relating to activity on the Internet). In the other Member States too, criminal prosecutions are an ***extreme rarity***, reserved for the most obstinate or crass law breakers such as companies which continue to maintain unregistered databases in spite of repeated warnings, or which export data in spite of such warnings or formal notices, or people who knowingly flout the law by selling confidential personal information (e.g., policemen who obtain access to criminal records or other confidential information on behalf of unauthorised third parties).

We have seen above, at 12, that the availibility of such formal sanctions has **not** been effective in raising the overall level of compliance with general systems of registration of data

users or –operations - but this would seem to be the result, not of any inherent deficiency in the sanctions, but of a general reluctance on the part of the authorities to enforce registration in a heavy-handed way, or to devote resources to the chasing of non-registered data users.

Even so, the threat (perhaps even the silent threat) of sanctions does strengthen the hand of the data protection authorities in the course of their "discussions" with data user: they are used as a "**stick behind the door**" and greatly improve the authorities' "negotiating position". It is not unreasonable to say that in practice that is the main function of the available sanctions. One might add that in Germany on the other hand, in which there is perhaps greater awareness of and sensivity towards data protection issues than in some other countries, the absence of strong enforcement measures has not greatly weakened the hand of the authorities: in practice, "advice" or "warnings" (publicly!) issued by the authorities in that country are "almost always" followed - at least by the public-sector data users towards which the work of the German authorities is largely directed.

On the other hand, in some countries - notably Spain - the data protection authorities have, over the last few years, begun to enforce the law more strictly, by imposing ***very substantial fines*** of up to Euro 60,000.

The difference in formal powers - and perhaps just as much, the different ("softer" or "harder") approach to enforcement in the different Member States has caused **occasional problems**, as when an authority in one country which does allow the authority to ***order*** remedial action asked an authority in another Member State for cooperation, only to be told that the latter authority could do no more than ***urge*** or ***recommend*** the proposed remedial action.

The European data protection authorities have examined the scope of the powers of these authorities (and more in particular the power to carry out "audits") in the recently held "**Dublin Workshop**" (April 2002), which concluded (as will also be clear from the above) that there were again still **great divergencies** in this respect. Some of these - such as the need for judicial authorisation for certain sanctions in certain jurisdictions - relate to the national legal culture, and even to constitutional considerations. Rather than trying to harmonise such powers - which will be extemely difficult - the authorities should seek to agree **protocols** and **procedures** for ***mutual cooperation***, on the basis of a clear understanding of each others powers (and limitations).

As far as this study is concerned, it is equally important to note that the powers now vested in the data protection authorities, as currently exercised, have not been able to counter ***continuin widespread disregard for the data protection laws in the Member States***.

- o – O – o –

DK\Cambridge, September 2002