EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

COMPARATIVE STUDY

ON

DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS

Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28

WORKING PAPER No. 2:

Data protection laws in the EU:

The difficulties in meeting the challenges posed by global social and technical developments

Douwe Korff, London Metropolitan University

Submitted by:

LRDP KANTOR Ltd (Leader)
In association with

Centre for Public Reform

20 January 2010
(final [extended and re-edited] version)

CONTENTS OVERVIEW:

CONTENTS (in detail): page:

Continues overleaf

CONTENTS (in detail) (*continued*): page:

Continues overleaf

CONTENTS (in detail) (*continued*): page:

- o - O - o -

1. Introduction

This paper discusses the difficulties that arise if one tries to apply the main EC Directive on data protection (Directive 95/46/EC) and the data protection laws in the EU Member States that implement it, as currently drafted, to the new global social and technical context described in Working Paper No. 1. It does this by means of a comparative-legal analysis.[1]

Within the EU, both at European and national level, considerable attention has been given to the question of *how* the EU- and the national data protection rules apply (or should be applied) to many of the phenomena described in Working Paper No. 1, including CCTV,[2] RFID,[3] biometrics generally and DNA in particular,[4] telecommunications data,[5] and of course the Internet.[6]

While this attention has resulted in some very useful guidance, it has also illustrated the serious problems that arise when one tries to apply the rules in the Directive to these phenomena. Even basic questions, such as whether certain data related to these phenomena (such as IP addresses or communications traffic data) constitute personal data, or who, in a particular context, should be regarded as the controller of a particular processing operation, and who as a processor, are often not that easy to answer - and some interested parties may well challenge the views of national and European authorities in these regards (or ignore their guidance). The data protection principles, the criteria for lawful processing, the conditions for international data transfers, the information duties to which data controllers are subject, and the rights of data subjects - none are easily applied, implemented or enforced in the new environment, even if one accepts that they ought to, in principle.

Much less attention has been given to the, in some ways even more fundamental - and no less problematic - preliminary questions of *when* the EU rules, or rather the rules in the national laws giving effect to the EU rules, are applicable to these phenomena, and when they should not be applied; and to the question of *what* national law should be applied, and the extra-territorial- and conflict of law-issues that arise in this regard.

There is, moreover, the further crucial question of enforcement, of the realisation of the law in practice. Even if one can clarify *when the rules should be applied* and under *what* national law, and *how they should be applied* (under that law), the question still remains of how one can ensure *that they are applied* in practice. This touches both on the question of how individual data subjects (or perhaps groups of data subjects) can assert their rights, and on the more general question of how supervisory authorities can enforce the law (or are willing or capable to do so). Again, these are difficult enough matters in the current context; the pursuit of such private claims and official actions can become much more problematic in the new environment (although some matters, such as online subject access, can possibly be supported and made easier by the new technologies).

This paper discusses the difficulties that arise in each of these four respects. It starts with the preliminary questions: First, it examines when, in terms of the main EC Directive and the national laws implementing it, the rules in those instruments are applicable to the issue at hand, i.e. the question of what matters are (and are not) covered by the Directive and the national laws, or (wholly or partially) exempt from them. Next, it looks at the vexed question of which national law should apply (if any of them should): the question of "applicable law".

Third, it gives insights into the difficulties that arise when (once it has been decided that the rules apply in principle) one tries to actually apply the substantive standards of the main Directive to the new phenomena.

And fourth, the paper looks at the difficulties facing individual data subjects seeking to assert their rights, and the data protection authorities in generally enforcing the law, by first noting the defects in the current systems in these regards in practice and then discussing the yet greater difficulties that arise in the new environment.

Overall, this paper is therefore rather negative: it focusses on the difficulties, on the inadequacies of the European data protection regime.

In our final report, we will make more positive recommendations on possible ways to address these problems, on how to face the challenges.

2. The difficulties in determining *whether* EU data protection law applies to processing of personal data in the new technical global environment: the question of scope, exemptions and exceptions

This section will deal with the first preliminary question that must be answered before one can discuss how the rules in the Directive are to be applied in the new environment described in Working Paper No. 1. This concerns the scope of the Directive and of the national laws implementing it, and in particular the question of limits to and full or partial exemptions from these instruments. We will cover: the limitation of the scope of the Directive to matters within the scope of Community law and the exclusion "in any case" of (former) Third Pillar matters such as "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" (sub-section 2.1); the full exemption from the Directive of processing of personal data by a natural person "in the course of a purely personal or household activity" (sub-section 2.2); and the limited exemption relating to freedom of expression (sub-section 2.3).[7] In each case, we will first set out the rules in the Directive and then provide an overview of the way in which the Member States have dealt with these issues in their national laws.

The second preliminary question, dealt with in section 3, is about *what* national law should apply to a processing operation with an international (cross-border) aspect, once it has been determined that the issue falls within the scope of the Directive and/or the national laws implementing the Directive.

As shall be shown, there is an important link between these two questions, in that there are important ramifications if the combination of differences in the scope of the national laws, or in the size of the exceptions or exemptions in those laws, and the application of the "applicable law" rules in the Directive and the laws, result in some matters being given no protection, or less protection in the State which law applies than some other States might require. This is discussed to some extent at 2.3; we return to it, in relation to the Internet in particular, at 3.3.

In sub-section 2.4, we provide some provisional, tentative comments about how the issues in this section relate to the new environment described in Working Paper No. 1, and how the difficulties might be resolved.

2.1 FIRST AND THIRD-PILLAR MATTERS[8]

(a) The Limitation Of The Directive To First-Pillar Matters

According to Article 3(2), first indent, of the Directive:

> 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.

The Directive *as such* does therefore not apply to matters outside the scope of Community law and "in any case" not to (former) "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 former "First Pillar" of the EU). 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. Recent events, epitomised in the SWIFT, PNR and data retention controversies, have underlined the increasing use of personal data processed for private-sector purposes, for (former) Third Pillar purposes, and the impossibility of excluding the application of the Directive to processing of personal data for (secondary) law enforcement purposes.

Nor indeed should (former) Third Pillar processing be exempt from data protection rules or principles: that would violate Article 8 of the European Convention on Human Rights, which is increasingly applied by the European Court of Human Rights (and the European Court of Justice) in a manner that incorporates data protection principles and supports data protection law,[9] and thus also general principles of Community (and Union) law.

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);[10] and indeed a range of "Third Pillar" measures have addressed data protection, and data protection is now also ensured for processing by the Union itself. However, the relevant EU rules tend to focus on the EU-level databases and arrangements in respect of those databases:[11] There is, to date, little attempt to ensure harmonisation (or even approximation) of the national rules of the Member States in relation to policing, law enforcement, or national security.

As we shall see at (b), below, this causes problems in the transposition of the Directive into the laws of the Member States. And as discussed at 2.4, these problems will strongly increase in the new environment described in Working Paper No. 1.

(b) The Inclusive Scope Of The National Laws

From the point of view of the Member States, applying the requirements of the Directive only to matters within the scope of Community law creates problematic and unwarranted "seams" between data protection regimes in different (but not easy to separate) sectors.[12] It is therefore not surprising that the laws of almost 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 (former) "Third Pillar" matters such as police or state security. In a few countries (e.g., Denmark, Germany, Netherlands), such matters are dealt with, in whole or in part, in separate laws, but these still rest on the same basic (constitutional) principles as underpin the Directive and the general data protection law in those countries.

There is almost universal acceptance, within the Member States, that the principles in the Directive are formulated with sufficient flexibility, and subject to sufficient qualifications, to be applied to matters both within and without the scope of Community law, i.e., that there is no instrinsic need for the limitation in the Directive, restricting the scope of that instrument to matters in the former category only: that limitation is rightly seen as a technical requirement, simply stemming from the fact that the Directive, as an *EC* Directive, cannot apply to (former) Third Pillar issues. This was also the conclusion of an in-depth study by the author of the present paper, carried out for the Commission a decade ago:[13]

> ... 'seamless' implementation of the Directive, to matters both within and without the scope of Community law, is eminently 'feasible'. It would underline rather than undermine crucial constitutional requirements in many Member States. It would avoid the serious legal and practical problems which the 'seams' resulting from partial implementation would create. It would avoid possible conflicts between national constitutional and European legal requirements; and it would facilitate rather than hamper data exchanges relating to European matters outside of Community law such as, in particular, data exchanges in the context of intra-European police cooperation. It would achieve all that, moreover, without posing a hindrance to effective policing at the national or European level.

The Member States therefore do not feel that they need to follow the Directive in this regard, and they do not do so in practice.

Indeed, in many countries, it is a constitutional requirement that all processing of personal data - be this is in the private sector, the public sector, or special areas such as police and national security - be subject to adequate data protection rules. Failure to apply such rules to processing of personal data in any of such contexts would violate inviolable rights.

That is of course not to say that the principles should be applied in the same way in these different context - on the contrary, all Member States provide for extensive limitations, exceptions and exemptions in respect of specific requirements of the general data protection rules, when applied to law enforcement or national security issues (or to the main national bodies involved in these matters).

These special limitations, exceptions and exemptions need not be discussed here in detail.[14] It must be noted, however, that in this regard there is considerable divergence.[15] States have

fundamentally different approaches to such issues and, as already noted, there is little or no guidance at EU level on how to apply national data protection law to national police and national security issues. Rather, the most detailed and authoritative guidance is contained in a Council of Europe Committee of Ministers Recommendation, R(87)15, but this recommendation has no binding force and is far from fully complied with in the laws of the COE- or EU Member States.[16]

In some States, such as Germany, Italy and Spain, there are strict, and quite detailed constitutional-legal requirements that must be met (even if this is sometimes not fully achieved, or delayed for a long time, or only confirmed after challenges in the courts). In other States, such as the UK (where there is no written constitution or Bill of Rights, although the ECHR is now given internal effect), the legislator (which is largely controlled by the Government) feels free, and is still largely regarded as entitled, to exempt whole swathes of police and national security matters from any effective data protection rules. Most of the other Member States lie somewhere in between.

The issue is related to the question of "applicable law". Specifically, as further discussed in sub-section 2.3, an uncritical application, by a Member State, of the "applicable law" rules in the Directive, and of the rule on unimpeded transfers of personal data within the EU, can lead to the rights of some citizens being undermined in ways that will be constitutionally unacceptable to some Member States. These problems will moreover significantly increase in the new global technical environment described in Working Paper No. 1.

2.2 THE FULL EXEMPTION RELATING TO PERSONAL AND HOUSEHOLD ACTIVITIES AND THE DIFFICULTIES OF APPLYING THAT EXEMPTION TO "WEB 2.0"

(a) The Exemption In The Directive

Article 3(2), second indent, of the Directive fully exempts from its provisions:

> Processing of personal data ... by a natural person in the context of a purely personal or household activity.

From the text, it is not clear whether Member States are obliged to include a (full) exemption on these lines in their national laws: Article 3 of the Directive merely says that such processing is excluded from its scope. However, the recitals suggest the exemption is compulsory. Slightly redacted, Recital 12 says that:

> the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law, [but] the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses [should be excluded].

The exemption is mentioned here because its application (to which, until recently, little or no attention had been given) is becoming increasingly important in the new environment described in Working Paper No. 1, in particular in relation to "Web 2.0" - defined by the fact

that more and more of the "Web"'s contents are put out there by private individuals, through social networking sites such as FaceBook, "blogging", "twittering", etc.

The issue is well illustrated by the very recent Article 29 Working Party Opinion on social networking sites (SNS).[17] In this, it says, on the one hand, that:

> many users [of such sites] operate within a purely personal sphere, contacting people as part of the management of their personal, family or household affairs. In such cases, the Opinion deems that the 'household exemption' applies and the regulations governing data controllers do not apply.

The Opinion instead, understandably, focuses on the responsibility of the providers of such services, the hosts of such networks,, and on the secondary uses to which they might put the data uploaded to them by the users. However, the Opinion also "recommends" that users should only upload pictures or information about other individuals, with the individual's consent. For the purpose of this paper, the main question is whether the Directive, and the laws implementing the Directive, apply, or should apply, to the users of such services, and whether, in that case, they should be treated as controllers. The WP notes the changing nature of the activities of individuals in this regard; its analysis in this regard runs as follows:[18]

> A growing trend of SNS is the "*shift from "Web 2.0 for fun" to Web 2.0 for productivity and services*"[19] where the activities of some SNS users may extend beyond a purely personal or household activity, for example when the SNS is used as a collaboration platform for an association or a company. If an SNS user acts on behalf of a company or association, or uses the SNS mainly as a platform to advance commercial, political or charitable goals, the exception does not apply. Here, the user assumes the full responsibilities of a data controller who is disclosing personal data to another data controller (SNS) and to third parties (other SNS users or potentially even other data controllers with access to the data). In these circumstances, the user needs the consent of the persons concerned or some other legitimate basis provided in the Data Protection Directive.
>
> Typically, access to data (profile data, postings, stories…) contributed by a user is limited to self-selected contacts. In some cases however, users may acquire a high number of third party contacts, some of whom he may not actually know. A high number of contacts could be an indication that the household exception does not apply and therefore that the user would be considered a data controller.

A little later it adds: [20]

> When access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS or the data is indexable by search engines, access goes beyond the personal or household sphere. Equally, if a user takes an informed decision to extend access beyond self-selected 'friends' data controller responsibilities come into force. Effectively, the same legal regime will then apply as when any person uses other technology platforms to publish personal data on the web.

The Working Party here clearly leans in the direction of making users who upload material to a wide audience fully subject to the Directive, as controllers. Its opinion, read closely, states that "*If a user takes an informed decision to extend access [to any material s/he uploads]*

beyond self-selected 'friends"", that user becomes subject to the responsibilities of a data controller, and "*effectively, the same legal regime*" will apply to such a user as applies to a data controller. Indeed, it makes clear, in a footnote, that the same applies to "*publishing platforms that are not SNS*" and "*self-hosted software*."

In this, the WP relies also on the judgment of the European Court of Justice in Satamedia, in which the Court held that: [21]

> It follows that the latter exception must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals (see Lindqvist, paragraph 47). That clearly does not apply to the activities of Markkinapörssi and Satamedia, the purpose of which is to make the data collected accessible to an unrestricted number of people." (para. 44)

The WP rightly feels that this interpretation, too, suggests that the uploading of materials onto the "Web", by individuals using SNS or other means, with a view to disseminating these materials to "an unrestricted number of people", means that the "purely private" exemption does not apply. As the Court notes, this was already suggested by its Linqvist judgment. In that judgment, the ECJ had already ruled as follows:[22]

> As regards the exception provided for in the second indent of Article 3(2) of Directive 95/46, the 12th recital in the preamble to that directive, which concerns that exception, cites, as examples of the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, correspondence and the holding of records of addresses.
>
> That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.
>
> The answer to the third question must therefore be that processing of personal data such as that described in the reply to the first question is not covered by any of the exceptions in Article 3(2) of Directive 95/46.

The WP's basic approach is therefore not surprising. However, there are problems with its more detailed application. The first problem is that the criteria used by the WP to decide when to allow, and when not to allow, a user to rely on the exception are rather vague. Why would a "collaboration platform" for an association suddenly fall within the law when, presumably, a similar platform for an *ad hoc* group of people interested in a particular topic is not? When can it be said that a person "uses the SNS *mainly* as a platform to advance commercial, political or charitable goals"? If she promotes a new software application she designed, or a book she has written, on her page (amidst other matters)? If she discusses politics, or her involvement in Amnesty International, or Greenpeace? When do a large number of contacts become too high to be acceptable to the regulator? What does the WP mean by "knowing" a person, in the virtual world?

The second, consequent problem is that if the users are benefiting from the exemption, they are *not subject to any requirement* of the applicable law (or rather, in view of our later discussion of the question of "applicable law", laws) *at all*; they would for instance not need

to seek the consent of the data subjects whose information they upload. But if they were to not benefit from the exemption, they would be *fully subject* to the Directive, and to the laws implementing the Directive, and they then would need such consent. This distinction thus has major impacts. It cannot be left to the crossing of ill-defined lines as suggested by the WP.

The overall problem is that the granting of a full exemption from data protection requirements to anyone who uploads materials to the Internet as a private individual would lead to easy circumvention of the rules and, in an age of user-generated content, would fundamentally undermine data protection (and privacy) itself; yet the full imposition of the law to all such individuals would seem excessive and, because of the sheer numbers, would be largely unenforceable.

The question - the challenge - is then perhaps whether a middle way be found? And if so, whether that would require a change in the text of the Directive(s) (and the national laws)?

The issue is likely to become more pressing if, in a truly developed "Web 2.0" environment, social networking will come to rely less and less on special, commercial service providers. If such networks can begin to grow "organically", without being explicitly hosted by a commercial entity, the current main target of the WP's regulatory attention would evaporate; and many of us - and most young people - would, in theory, have to conform to all the requirements of the national data protection laws in respect of their online "social network" activities.

(b) The Exemption In The National Laws

The exemption for "purely personal" processing is repeated, with minor, unimportant variations, in most of the national laws of the EU Member States studied. Like the exemption in the Directive, until fairly recently, these exemptions were given little or no attention in practice. Individuals carrying out minor processing operations, for themselves, were basically left alone, if not expressly on the basis of this exception than because of the principle *de minimus non curat lex* (the law does not deal with trivial issues).

Recently, however, "blogging" and social networking sites have attracted the attention of the national data protection authorities. According to the WP: [23]

> In several Member States, the lack of access restrictions (thus the public character) [of some SNS data] means the Data Protection Directive applies in terms of the internet user acquiring data controller responsibilities.

It may suffice to illustrate this with reference to the approach of one country, France, to the issue of social networking and "blogging" on the Internet.

The national data protection authority, the CNIL, has issued a brief comment, *Facebook et vie privée, face à face*, on its website, summarising a more elaborate Recommendation.[24] This (like the Article 29 Working Party Opinion) focusses on the responsibility of the SNS service providers; it is silent on the question of whether users of such sites become subject to the law as controllers, for any personal data they upload and make available to others. However, the CNIL has made its basic thinking clear in the context of "blogs", under the

telling, if perhaps somewhat misleading heading "*Blogs: the [French Data Protection Law] applies, but [blogs] are exempted from the duty to be notified tothe CNIL*".[25] The exemption from notification is a technicality, mainly aimed at avoiding bureaucratic burdens (one suspects, on the CNIL as much as on "bloggers"). The crucial issue is the applicability of the law, and the implications of that view.

The CNIL discusses this in the following terms: [26]

> The dissemination over a website of information about individuals thus requires their prior consent. The individual [the data subject – DK] has the right subsequently to oppose this dissemination. The Recommendation draws the attention of those concerned [i.e., of "bloggers" – DK] to the fact that so-called sensitive data (for example, on [a person's] health or sexual orientation or politics) are not supposed to be disseminated over an Internet site. The CNIL advises Internet users who create a personal website for a circle of family or friends to impose access restrictions. If someone sets up a website for those close to him in order to put photographs of an event (such as a marriage or anniversary, etc.) online, he must limit the dissemination [of those photographs] to those concerned only. ... As far as the collection of personal data is concerned, the Recommendation recalls that individuals from whom those are collected must be informed of the purpose of the collection, the recipients of the data and the existence of a right of access, correction and objection. The retention period must be proportionate to the aim of the website, and the data may only be disseminated to third parties within the context of private activities, and subject to the data subject [the person whose photographs or data are disseminated – DK] being informed of this and given the opportunity to object to it.

This is somewhat ambiguous, but basically in line with the WP Opinion. Clearly, dissemination of personal information by a "blogger" - and, one may assume, by a user of a social networking site - is subject to the law if the data are made available to all but a small, clearly-defined, personal circle. Without expressly saying so, the CNIL suggests that, by contrast, dissemination to a very small personal group of family or friends would not be subject to the law, i.e. would benefit from the "purely personal processing" exception.

Clearly, in France, and increasinly in many other EU Member States, the exception is therefore, in this context, very strictly (and restrictively) applied, to really purely personal distribution of personal information only.

However, this approach has not been universally adopted. In the UK, the data protection authority (the Information Commissioner's Office or ICO) has looked at social networking sites, and issued guidance[27] - but this notably ignores the issue addressed by the WP and the CNIL: if and when ordinary users uploading information on other individuals might become subject to the national data protection law (in the UK, the Data Protection Act).

In fact, it would appear that the ICO has not yet even addressed the responsibilities of the SNS service providers. And as far as users are concerned, it has restricted itself entirely to issuing guidance to individual (in particular, young) SNS users, warning them against uploading too much information on themselves. Astonishingly, the guidance does not even mention the issues that arise if a user uploads and disseminates information on other individuals.

This may serve to underline the serious discrepancies that exist in this regard between the Member States. Some are very strict, and treat many users of SNSs as controllers, while some others largely ignore them, beyone advice to be careful.

Another problem is that users of social networking sites move, physically. One day, they may be uploading information (including personal data, like photographs) on (of) others from London; the next day, they may be in Madrid, or Prague, or New York, or Beijing. Little attention has been given to this by the DPAs.

In addition, the question of uploading information to the "Web" is of course also part of the freedom to "seek, receive and impart information", discussed under the next heading. The use of SNS, "blogging", etc., is a major issue to be addressed in the new global technical environment described in Working Paper No. 1. The above information shows how big the challenges in this respect are.

2.3 THE LIMITED EXEMPTION RELATING TO FREEDOM OF EXPRESSION AND THE DIFFICULTIES OF APPLYING THAT EXEMPTION TO "WEB 2.0"

(a) The Exemption In The Directive

Similar, indeed in some way even more profound difficulties than the ones just discussed arise in respect of another, more limited exception, contained in Article 9 of the Directive which stipulates the following:

> 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.

The Directive does not provide any guidance on what is "necessary" in this regard; the most important guidance in this respect would in any case derive, not so much from the Directive as from the European Convention on Human Rights and the case-law of the European Court of Human Rights under Article 10 of the Convention.[28]

The Article 29 Working Party selected the issue of "Data Protection and the Media" as the very first topic it ever addressed, as long ago as 1997.[29] However, perhaps because of the major difficulties the topic raises, it has not returned to it since. Suffice it to note that in its Recommendation, the WP basically concluded, on the question of balance, that:

> Data protection law does in principle apply to the media. ... [and that]
>
> Derogations and exemptions under article 9 must follow the principle of proportionality.

This does little to clarify the exact limits of the exemption.

We will not discuss here in general the difficult question of how to balance the right to privacy and the right to freedom of expression, other than to note that under Article 10 of the

European Convention on Human Rights (and Article 11 of the EU Charter of Fundamental Rights) the latter explicitly includes the freedom:

> to receive and impart information and ideas without interference by public authority and regardless of frontiers.[30]

More important in the present context are two other matters. First of all, both rights (privacy and data protection, and freedom of expression and freedom to seek, receive and impart information) are fundamental rights, strongly protected in the constitutional laws of many Member States. Often, the precise limits on freedom of expression generally, or *versus* the right to privacy or informational self-determination, are very specific to a particular Member State (even if all Member States subscribe to the same basic principles in these regards). One need only mention holocaust denial, blasphemy, incitement to religious or racial hatred, support for terrorist organisations or causes, pornography, publication of details of the private or sexual life of public figures or "stars", etc. etc. There is no uniformity in the law in this regard. In the case-law of the European Court of Human Rights this is recognised and accepted, in the sense that States Party to the ECHR are granted a "margin of appreciation" in the application of the provisions of the Convention, and in the limitations they feel they need to impose.[31]

The ECJ, in its Linqvist judgment, equally stressed the discretion that the Directive and the ECHR grant to the national authorities in the Member States (legislative and judicial) to find the right balance between these sometimes conflicting rights; to quote the most salient phrases:[32]

> ... in many respects, the Member States have a margin for manoeuvre in implementing Directive 95/46.
>
> ... it is ... at the stage of the application at national level of the legislation implementing Directive 95/46 in individual cases that a balance must be found between the rights and interests involved.
>
> [in the case at hand], in essence, Mrs Lindqvist's freedom of expression ... and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site.
>
> Consequently, it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with Directive 95/46 but also to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order [read here, in particular: the right to freedom of expression and to freedom to receive and impart information – DK] or with the other general principles of Community law, such as inter alia the principle of proportionality.
>
> It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order [which include both data protection and the right to freedom of expression - DK].

The Court therefore concluded that Directive 95/46/EC, while it restricted the right to freedom of expression (including the right to receive and impart information), did not violate that right, precisely because it could be sufficiently flexibly applied, and under Community law must be implied in a manner consistent with the ECHR. It was up to the national court to determine how in any particular case (and in the particular case of Linqvist) the balance between freedom of expression and privacy should be struck, provided two requirements were met:

- ✓ The national court should not simply apply the rules in the Directive if those impacted on the right to freedom of expression and freedom to receive and impart information without further ado, but rather, should take that latter right into account - if needs be, that right could be relied on to disapply rules in the Directive and/or in the national law given effect to the Directive; and

- ✓ Any such national decision would have to be proportionate (read: in relation to both rights).

The Linqvist judgment therefore emphatically did *not* say - or even imply - that the dissemination of information on a person on a website (even of sensitive information), without that person's consent, should be prohibited in all Member States on the basis of the Directive. Rather, the Court ruled that the Directive applied, and that it in principle imposed that obligation. But it also recognised that this duty had to be balanced, in each individual case, against the right to freedom of expression and freedom to receive and impart information. It then left it to the national courts to decide whether, in a particular case, the requirements of the Directive should be applied, or whether they should be disapplied or relaxed in order to protect freedom of expression.

And (to return to our main topic), the Court also accepted that the courts in different Member States might strike this balance differently in otherwise comparable cases: that is inherent in the "margin of appreciation" doctrine applied by both the ECJ and the European Court of Human Rights.

As such, this is relatively basic European law. However, the application of these principles becomes more difficult in the new global technical environment described in Working Paper No. 1.

Specifically, serious problems are created if, as a result of the "applicable law" rules in the Directive, fundamental constitutional-legal human rights standards of a particular Member State were to become inapplicable or unenforceable, and if the Directive's rules would thus deprive citizens of that State from those rights, because the matter were to fall under the law of another country which does not grant the right to the same extent (even if that other country is also an EU Member State and thus also a Party to the European Convention on Human Rights). It could revive the old "*solange*" problem about the supremacy of Community law, not just in Germany (where the issue was raised by the Constitutional Court), but also in other countries with strong constitutional human rights protection. We will return to this in sub-section 2.3.

Secondly, Article 9 of the Directive is manifestly too restricted, in that it only appears to envisage special exemptions for journalists, artists and literary authors (for "*processing of*

personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression"). By contrast, Article 10 of the European Convention on Human Rights guarantees the right to freedom of expression - including the right to seek and receive information without interference and regardless of frontiers - to *everyone*.

If the special exception in Article 9 of the Directive were to be applied restrictively by a Member State, to journalists, artists and officially recognised "literary" or "professional" writers only (whatever those might be), that would manifestly violate Article 10 of the Convention - and thus general principles of Union law. Yet as we shall see below, at (b), that is exactly what is being done in some Member States.

This issue too will become increasingly important in the new environment described in Working Paper No. 1, and in respect of "Web 2.0" in particular: in the new environment, and in particular on the Web, the dissemination of information - including information of public interest - is no longer a matter for a special, selected caste. On the contrary, "Web 2.0" will be dominated by user-generated content, by information "imparted, sought or received" by non-professionals - in particular, but not only, through the social networking sites discussed earlier. The "twittering" surrounding recent events in Iran following the contested election there in June 2009, is a good example of this new reality. In this new context, Article 9 as currently drafted is manifestly deficient.

The two issues are furthermore linked: It will not be acceptable in some, indeed many Member States - indeed, it will in some (like Germany) be *constitutionally impossible* for them to accept - that the limits of freedom of expression and the freedom to seek, receive and impart information (especially over the Internet) of their citizens were to be determined by the laws of other Member States, if those foreign laws were to restrict those freedoms in ways and to extents that would not be permitted under their domestic constitutions, e.g., because they would apply Article 9 of the Directive only to officialy recognised journalists etc. (or indeed, in some cases - such as holocaust denial or incitement - if the laws of the other countries failed to impose restrictions on freedom of expression deemed essential in the first States).

The question of "applicable law" is therefore a particularly sensitive one in this context. And as we shall see, the national laws as currently drafted notably fail to resolve the problems.

(b) The Exemption In The National Laws

The tension between data protection law and the law on freedom of expression, and the freedom to seek, receive and impart information without interference, regardless of frontiers, is a crucial, but also very difficult issue in any democratic society. What is more, the balance is not struck in the same way in different countries; indeed, some States have given this much more careful consideration than others. This means that the exemption in the Directive is applied quite differently in different Member States: some have quite deliberately extended the exemption to try and fit in with the broader provision of the ECHR; some have done so partly, but not very succesfully; and some have given the issue scant regard altogether, and just copied the wording from the Directive. The wide scope of different approaches can be sufficiently illustrated by reference to the Summary of National Laws, prepared by the author of this paper for the Commission in 2002; the laws in the States that

have joined the EU since then fit within the same range. The 2002 study found the following:[33]

The need to extend the exception related to freedom of expression to everyone (and not just to journalists, artists and artistic writers) is recognised particularly clearly 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 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."*[34]

Such considerations are not only of particular importance to human rights organisations , who collect sensitive data for purposes which are not solely "journalistic" in a narrow sense. They are also crucial in the new global-technical environment described in Working Paper No. 1, and more specifically in relation to user-generated content on "Web 2.0".

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 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."

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 on the 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.
>
> 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 in hard copy, which was beyond its competence: the annual report in that format was not to be considered 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 in sub-section 2.2, below. 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".[35]

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 then 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). The 2004 data protection law confirmed and extended these exemptions, and added exemptions with regard to processing for the sole purposes of literary or artistic expression. It exempts 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 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 factually correct but nevertheless damaging 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 held 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 might 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.[36] 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 cases, 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 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 (a previous Data Protection Registrar 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.[37] However, the judgment in Naomi Campbell –v- the Mirror Group of Newspapers - 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.[38]

The Irish law contains an almost identical exemption, and may therefore 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 Internet, 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 Internet 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".

One question is whether the terms used ("journalistic", "artistic", "literary", "the press", "the media") include purely factual publications, such as directories; presumably, they do not.

A further point which may be noted is the problematic involvement of the data protection authorities in media 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.

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, for the benefit of everyone, through wide exemptions for the press (but not for non-professionals), 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, and yet others would leave the issues to the courts. This is clearly an area in which no serious convergence can be discerned, either in substance or in terms of procedure or forum.

More important for the present purpose, is the apparent exclusion of "non-professionals" such as SNS users, "bloggers" and "twitterers", in some but not all Member States, from the benefits of the exemption. As noted earlier, these are precisely the people who, in the new global-technical environment of "user-generated content", will provide most of the information to the public. Their exclusion from the exemption may in many cases violate the European Convention on Human Rights and thus general principles of Union law.

What is more, such exclusions in some Member States - which can amount to undue restrictions on the rights of such individuals to freedom of expression and freedom to disseminate information in those States – can also contravene constitutional requirements in some other Member States. As already noted, this would mean that those other Member States will find it constitutional difficult - if not impossible - to defer to the application of the laws in the first kind of States.

Similar problems could arise out of the application of laws which unduly restrict freedom of expression of non-EU citizens (by not extending the exemption to them), if those non-EU citizens were to become subject to such laws. This applies especially to US citizens, who in their domestic law are given very strong, and wide, protection of their right to freedom of expression and dissemination of information. Imposition of restrictive EU rules on websites of US webhosts, in this field, would be highly contentious.

In the next section, we will examine the rules in the Directive which could lead to such problems.

3. The difficulties in determining *what* national data protection law applies to processing of personal data in the new technical global environment: the question of "applicable law"

The question of "applicable law" has been one of the most vexed ones brought up in relation to data protection in Europe. The issue goes back all the way to the drafting of the main EC Directive on data protection, and before.[39] It is further complicated by the fact that it is not just that the rules in the Directive are complex and difficult to apply, but that on top of that, the national laws implement those rules in different ways.

The provision on this matter in the Directive hinges on two main rules: one relating to controllers established in the EU, and one for non-EU controllers. We will examine these in turn, in sub-sections 3.1 and 3.2, and then look at their application to the Internet, in sub-section 3.3. As before, we will each time address first the rule or rules in the Directive (at (a)), and then the way in which they have been implemented in the laws of the Member States (at (b)).

As in the previous section, we provide some tentative, provisional comments at the end, in sub-section 3.4.

3.1 THE SITUATION CONCERNING CONTROLLERS ESTABLISHED IN THE EU[40]

(a) The First Main Rule In The Directive

The European Commission, which drafted the directives, recognised that the existing data protection laws in Europe clashed in various ways and, therefore, from the beginning included a special provision in the (then draft) main data protection directive on the question of "applicable law": Article 4. Earlier attempts to resolve this issue at the international level—in particular, in the context of the drafting of Council of Europe Convention No. 108—had failed[41] in spite of, or perhaps because of, a whole range of different solutions having been suggested by academics.[42]

The aim of Art. 4 of the main Directive (which also determines the territorial applicability of the e-Privacy Directive) is quite clear. As the Commission put it in its Explanatory Memorandum to the Amended Proposal:[43]

> This article lays down the connecting factors which determine which national law is applicable to processing within the scope of the Directive, in order to avoid two possibilities:
>
> - that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this;
>
> - that the same processing operation might be governed by the laws of more than one country.

Leaving aside the question of non-EU-based data users (discussed at 3.2), the original and amended Commission proposals were quite straightforward on the question of applicable law. The original proposal stipulated quite simply that:

> 1. Each Member State shall apply this Directive to:
>
> (a) all files located in its territory; ...

The Amended Proposal had to be changed somewhat to reflect the change of the core concept in the Directive from "file" (structured filing system) to "processing" (processing operation). The text of Article 4 of the Amended Proposal otherwise retained the simple "country of origin" rule of the original proposal and read:[44]

> 1. Each Member State shall apply the national provisions adopted under this Directive to all processing of personal data:
>
> (a) of which the controller is established in its territory or is within its jurisdiction; ...

At the very last minute, however, the Council changed this still relatively straightforward language to a much more convoluted text, which became the final wording and which reads as follows:

> 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 in 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; …

This difficult provision has been analysed in some detail elsewhere.[45] Here, it may suffice to note that the aim of the provision is still to ensure that, in principle, any one processing operation within the EU should always be subject to one national law of one Member State only (and never to no such national law, or to more than one such law).[46] However, there are problems in this regard, even with the text of this provision itself (further problems, arising from divergent implementation of the provision in the national laws, are discussed separately, below, at (b)).

Specifically, the application of Article 4 rather confusingly turns on two concepts and a practical question: the concept of "controller" and the concept of (an) "establishment," and

the question of when a processing operation can be said to take place "in the context of the activities of" a specific, identified "establishment."

Thus, in order to determine whether the law of a particular country applies to a particular processing operation, it is necessary to clarify:

- ✓ first, exactly what processing operation is under consideration;
- ✓ second, who the controller of the operation is;
- ✓ third, what "establishments" of this controller are involved in the operation and where they are based; and
- ✓ fourth, in the context of the activities of which of these establishments the processing can be said to be taking place.

Let us look at each of these in turn.

"*[a] processing [operation]*":

The term "processing" is used in the Directive as both a verb and a noun, which causes some complications. First of all, the verb "processing" (to process) is defined in Article 2(b), as follows:

> '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.

Clearly, this is a comprehensive term: it covers literally any action taken in respect of personal data, from their initial collection, through their storage, manipulation and use (including internal dissemination and external disclosure), to their archiving, "blocking", deletion or destruction.

But the term is also used as a noun, as in the definition of a "controller" as the person or body which "alone or jointly with others determines the purposes and means of the processing of personal data" (Article 2(d)). In that sense, it is often better, at least in English, to think of the term as referring to a "processing operation"; those words are in fact used in Article 17, concerning notification.

It is also basically in that latter sense, that one can best read the word "processing" in Article 4(1), where (as we have seen) this stipulates that

> Each Member State shall apply the national provisions it adopts pursuant to this Directive 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

Processing operations in this sense are essentially defined by the purpose or purposes they serve: one can think of processing for marketing purposes (Art. 14(b)), or for scientific research purposes (Art. 13(2)), or for certain medical purposes (Art. 8(3)). For the proper application of the Directive, it is crucial that such purposes are narrowly defined: the more

sweeping a definition one uses of the purposes of "processing" (i.e., of certain processing operations), the less protection is accorded to the data subject. The Directive already provides for flexibility in that it allows for secondary processing, not only for the main, primary purpose for which data are collected, but also for "compatible" purposes (cf. Article 6(1)(b)).[47] That the primary purpose must, in return, be narrowly defined is made clear by the requirement that that purpose must be (specifically) "specified" (*idem*). It is also implied in the reference in the provision on notification (art. 18) to a "processing operation or set of such operations intended to serve a single purpose or several related purposes".

Thus, for instance, Article 8(3), just mentioned, refers to processing for:

> the purpose**s** of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services

Processing of personal data for the purposes of medical diagnosis and treatment is therefore distinct from processing of such data (indeed, of the same data) for the purpose of preventive medicine, and even more distinct from processing for the purpose of health-care services management. The processing of the same data may, in this context, well serve "related purposes"; indeed, those purposes may, to some extent, be "compatible". But that does not mean that the different processing operations should not be strictly distinguished: only then can the Directive be properly applied. For instance, it is only if one makes such distinctions that one can clarify exactly what data, in what form, can be used for each purpose. Thus, e.g., for many administrative and management purposes, patient data may well have to be anonymised or at least pseudonymised. Indeed, while some medical details may have to passed on to care staff, this need not involve disclosure of a patient's complete medical records. Etcetera. It may also be noted that the list in Article 8(3) does not include scientific research: that is clearly a distinct purpose, and any use of patient data for such a purpose is therefore even more obviously separate from the primary use of treatment.[48]

For the present analysis of the rules on "applicable law", it is important, in any transnational context, to clearly distinguish different processing operations, especially within a complex, internationally operating organisation. For instance, the processing of personnel data for tax and social security purposes should be distinguished from the processing of such data for internal staff review and promotion purposes, etc.. In such complex organisations, this is often far from easy.

"*controller*":

The controller is the legal or natural person who "determines the means and purposes" of the processing (Art. 2(d)). However, the Directive complicates this by saying that the controller can make this determination "alone or jointly with others" (*idem*). This could be read as suggesting that for some operations, there can be "joint controllers" - but that would seriously complicate the "applicable law" determination, if there were "joint controllers" based in different countries. Perhaps a better reading would be that there still always is only one controller for any specific processing operation, who may however involve others in making the determinations about means and purposes (perhaps especially the means). But

that could be read into the text without the added stipulation. The concept is further discussed in the next section, at 4.1, below.

"*establishment*":

The term "establishment" refers to a "stable arrangement" used for the "effective and real exercise of activity" (19th Preamble). This is line with general rules of Community law, as interpreted by the ECJ.[49] The "stable arrangement" can be an office kept in the country concerned in the name of the controller himself, a branch office, or a subsidiary, or a wholly or partly-owned company: "*the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect*" (*idem*). Rather, the determining factor is whether the controller makes (real and effective) use of the "establishment" in its (i.e., the controller's) processing operations. The establishment has to be an establishment *of* the controller: An agent used on an *ad hoc* basis is not an establishment of the controller but merely a "processor" (although if the arrangements between the controller and the agent become quasi-permanent, this could change).

In this regard, the Article 29 Working Party made the following comment:[50]

> When the same controller is established on the territory of several Member States, each of the establishments must comply with the obligations laid down by the respective law of each of the Member States for the processing carried out by them in course of their activities. It is not an exception to the country of origin principle. It is merely its strict application: where the controller chooses not to have only one, but several establishments, he does not benefit from the advantage that complying with one law is enough for his activities throughout the whole Internal Market. This controller then faces the parallel application of the respective national laws to the respective establishments.

The Working Party said it might want to come back to this issue, but it has not yet done so.

"*in the context of*":

In fact, the situation is in reality already much more complex, in particular in relation to the fourth issue: whether a processing operation takes place "in the context of the activities" of a particular "establishment". The WP29, in its Working Paper, did not really address this issue. Rather, it envisaged a controller with different establishments that each operate more or less independently, even if perhaps under some central guidance.

In practice, the operations of different entities within a multinational company or organization will often vary: some operations may be under the direct central control of the international (European) headquarters of the group, and some may be under the control of the local establishment. Even that may often not be clear. For instance, one would normally assume that personnel (employment) records are "local", i.e. that they are processed in the context of the activities of the local establishment, and that that local establishment is therefore the controller. However, many multinational companies or organizations regard all the group's employees, worldwide, as "theirs"; promotion and training, posting and other arrangements (such as medical care and pensions) may be centrally directed and controlled. And such control will often extend to the processing of the personal data of the employees

involved - or more specifically, to the determination of the "means and purposes" of that processing.

On the basic assumption of local control, under the terms of Article 4, (only) the national data protection law of the local establishment would apply to the personnel records of the people employed by that local establishment. But if the second scenario applies, one could feel that not the local establishment, but the central office is the controller, and that the local establishment merely acts as a processor on behalf of its central office when it processes data on people who are employees of the group. In that case, arguably, the law of the (EU) country where the head office is based would apply to all processing of all personnel data on all the group's employees, in all EU Member States (and none of the local data protection laws in the other EU Member States apply).

It is thus already in practice far from easy to determine the above-listed matters in respect of complex, multinational companies or organizations or groups of such entities, even if their operations are entirely confined to the EU area. Often - e.g., in respect of employment data, or customer data - it is difficult to determine which specific establishment in which country, which is somehow part of such a complex entity or group of entities, is the controller of a particular operation, and who a processor.

The problems are compounded in the new environment described in Working Paper No. 1, especially (but not only) in relation to online activities - again even if all these activities are limited to EU Member States. Companies and organizations can have a "presence" in several Member States, and operate in the virtual world in these and other Member States. In operational terms, some companies will treat all their operations, at least throughout the EU, as one. Other companies have operational areas that cross State boundaries, with (e.g.) one regional centre responsible for all Scandinavian operations, one for all German-speaking areas (Germany, Austria, the German-speaking part of Luxembourg - and often also the German-speaking Swiss cantons), one for Spain and Portugal, one for the Benelux, one for the UK and Ireland, etc. Such arrangements are common, indeed typical. The different entities can have different degrees of operational freedom, or different degrees of freedom in relation to different types of operations (including personal data processing operations). Databases used by any, or some, of the relevant entities may be situated in other entities belonging to the group. Some of the data from some entities may be shared with other entities, or with the central entity (the European headquarters). Such groups may also have have separate (but linked) arrangements for their on- and offline activities.

All of these matters affect the answers to the above questions as to which entity must be regarded as the controller, in respect of different processing operations by different establishments - and thus what law applies to those operations. Very often, the answer will differ according to the operation. This means that, on paper, and even within the EU, for purely intra-EU (but still transnational) processing operations, corporate or other entities that belong to a larger group must often comply with different data protection laws in respect of different processing operations they carry out: they must conform to the requirements of their own national data protection law when it comes to processing of personal data carried out in the context of their own activities, but they may have to comply with data protection laws of other EU Member States in respect of processing of personal data on behalf of other group entities, in particular their headquarters.

In this sub-section, one further matter may be noted. This is that the rules in the Directive require the EU Member States to apply their laws not just to processing of personal data on individuals on their territory. On the contrary, the Member States must apply their national data protection laws to any processing carried out "in the context of the activities of an establishment of the controller on the territory of the Member State". The words "on the territory of the Member State" here refer to the "establishment" in question, and not to the activities. This is clear from the other language versions of the Directive (e.g., from the German one), and from the subsequent sub-clause about controllers with establishments in different Member States. This means that all Member States must apply their national data protection law extra-territorially, to processing of personal data on anyone, anywhere in the world, if this is done "in the context of the activities of" an establishment in their territory. This clearly includes all data collection on all visitors to the website of an EU-based company, irrespective of the place where the visitors are, and also all collecting of personal data in another country, by an EU-based controller, directly from the data subjects, e.g., by 'phone or by means of questionnaires sent to them, and presumably also to such collection, in the other country, of personal data by a "processor" on behalf of the controller in the first country.

As the Article 29 Working Party put it in a Working Document on the application of the Directive to the Internet (discussed in more detail later, at (c)): [51]

> It is worth noting that it is not necessary for the individual to be an EU citizen or to be physically present or resident in the EU. The directive makes no distinction on the basis of nationality or location because it harmonises Member States laws on fundamental rights granted to all human beings irrespective of their nationality. Thus, in the cases that will be discussed below, the individual could be a US national or a Chinese national. In terms of application of EU data protection law, this individual will be protected just as any EU citizen.

And even more clearly in its Opinion on search engines:[52]

> It is important to note that in this case [when a search engine provider is situated in a Member State], data protection rules are not restricted to data subjects on the territory or of a nationality of one of the Member States.

(b) The First Main Rule In The National Laws

The laws in some Member States (e.g., Netherlands, Portugal) use the exact phrase used in the Directive to implement the latter's first main rule on "applicable law", i..e., they apply to "processing carried out in the context of the activities of an establishment of the controller on the territory of" the Member State. Some others also closely follow the Directive, with some elaboration, but with that elaboration also being in accordance with the Directive (e.g., Austria, Belgium). Many others use slightly different or slightly more complex terms, but which still effectively fully accord with the requirements of the Directive in this respect (e.g., France, Greece, Ireland, Luxembourg, UK, Sweden).

However, the laws in some Member States do not appear to fully or properly implement the rule. Sometimes, the differences would seem relatively small, and can perhaps be resolved by interpretation. Thus, the law in Finland refers to "processing of personal data where the

controller's establishment is situated on the territory of Finland"; and the Spanish law applies to "processing [which] is carried out on Spanish territory as part of the activities of an establishment of the controller". Somewhat further removed from the text of the Directive, the Italian law stipulates that it applies to "processing of personal data, by anyone, carried out on the territory of [Italy]".

The law in Denmark applies the first main rule correctly in respect of activities by a Denmark-based controller, but only if those activities "are carried out within the territory of the European Community" (Art. 4(1) of the Law). In other words, it would seem to fail to apply its data protection law to processing (e.g., collecting) of personal data by a Denmark-based controller in non-EU countries.

The German law disinguishes between processing in Germany by a controller established (*belegen*) in another EU State, without this involving an establishment (*Niederlassung*) of the controller in Germany, and processing in Germany by a controller established in another EU State but which is carried out by an establishment of the controller in Germany. The law does not apply in the first situation, but does apply in the second situation.

The first rule appears to not cover the (not uncommon) situation in which an establishment in Germany of a controller from another EU 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 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 appears to suggest that contrary to this, it (the German law) applies, but can perhaps in this respect be interpreted in accordance with the Directive.

Conversely, 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 is carried out in another EU State by an establishment of a German controller in that other EU State, but in the context of the activities of that latter establishment? According to the Directive, it should in that case be the law of that other EU State that applies and not the German law - but the law is silent on this.

The same issue arises *a fortiori* under the Greek law, which applies to "processing by a controller established on the territory of Greece", and under the Swedish law, which applies to "controllers of personal data who are established in Sweden", in both cases without reference to the processing having to take place "in the context of the activities of" the establishment of the controller in question.

These imperfections in transposition could have ramifications, in particular in view of the fact that almost no national law - including the national laws of the countries just mentioned: Finland, Greece and Sweden - expressly state that they do <u>not</u> apply to processing carried out on their territory or in respect of their citizens if the processing takes place in the context of an activity of an establishment of the controller that is not situated on their territory but in another EU Member State (say, in France, or Germany, or the UK).

One of the countries whose law does spell out this limitation on its applicability is Belgium. Indeed, the Explanatory Memorandum to the Belgian law even usefully adds that, in cases in which the law of another EU Member State applies to processing by a Belgian controller, this 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 gives effect to 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".

3.2 THE SITUATION CONCERNING CONTROLLERS NOT ESTABLISHED IN THE EU

(a) The Second Main Rule In The Directive

The situation concerning controllers who are not established in the EU is more problematic: According to the Directive, every Member State must apply its national law to processing operations by such non-EU companies if the processing involves the "mak[ing] 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 [the EU] (Art. 4(1)(c)).

The broad term "equipment" would appear to cover any computer (including portable PCs or even mobile 'phones, especially if they are web-enabled), computer system, mainframe, or even switching or holding systems used to store or transfer data (except for systems only used to transfer data through the territory of the EU, without retaining a copy).[53]

It would also appear that if *any such equipment* is used in the EU, for *any aspect* of a processing operation (other than mere transit through the EU), *each* of the Member States in which such equipment is used must apply *all* of its data protection law to *all aspects* of that processing operation. Of course, in a transnational processing operation involving several Member States, equipment in each of these States is likely to be used.

For non-EU controllers involved in such operations, the Directive would, therefore, appear to have the opposite effect as it seeks to achieve for EU-based controllers: rather than eradicating conflicts of law and the concurrent application of different national laws to single processing operations, the Directive creates them. In addition, such controllers would have to appoint several "representatives" in the EU: one in each Member State where they "use" equipment (Art. 4(2)).

In practice, as we shall see under the next headings, the Article 29 Working Party and the national data protection authorities take a "cautious", "pragmatic" view, and are not aggressively enforcing all the laws all of the time. But that is not really an answer to the problem: it leaves companies - and data subjects - unclear about their duties and rights.

(b) The Second Main Rule In The National Laws

The rules and requirements of the Directive, discussed at (a), are basically applied as stipulated in the Directive in most of the Member States, including Denmark, France, Greece, Italy, Luxembourg, the Netherlands, Portugal, Spain and Sweden (albeit with some minor textual variations). However, there are some more significant differences between the Directive and the national laws in some other countries.

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".[54] "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 (Austria, Denmark, Germany) do not contain any reference to "equipment" or "means" in their laws in this respect at all. As we shall see below, at 3.3, this wide application of the term "means"/"equipment" is also broadly adopted by the Article 29 Working Party, especially in relation to the Internet.

Secondly, 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 Danish, Italian and Portugese laws. The French and Luxembourg laws refer to transit through [French/Luxembourg territory] or through [the territory] of another Member State of the European Union, which amounts to the same thing. The same applies to the Swedish law, which applies the exception if the equipment "is only used to transfer information between a third country [i.e. a non-EU country] and 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.

Moreover, some Member States apply their law to non-EU controllers even more widely than as suggested by the Directive, or apply specific formalities more widely. Specifically, the Austrian and Greek laws 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 (although this requirement is apparently being removed). It must be stressed that, on their face, these provisions appear to apply also to controllers in 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. The provision is also problematic in relation to activities on the Internet, as discussed below, at 3.3.

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 divergencies between the laws of the Member States. As a result, some positive and negative conflicts of law remain between the Member States; and the treatment of non-EU based controllers differs.

Some of these problems can be resolved 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) once said:

> 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.

3.3 APPLYING THE RULES IN THE MAIN DIRECTIVE TO THE INTERNET

(a) Applying The "Appliable Law" Rules In The Directive To The Internet

The Article 29 Working Party has given extensive attention to the application of the EU rules to the processing of personal data on (or in relation to activities on) the Internet.[55] The question of when, under Article 4 of the main Directive, the national data protection laws of the EU Member States apply (or at least should apply) to such processing, was addressed in most detail in Working Document WP56 (already mentioned).[56] The WP has since confirmed

the approach in that document in its opinion on search engines and the subsequent rules on processing of IP addresses and the use of "cookies".[57]

It is notable that the WP Working Document is strongly assertive about the extra-territorial application of the EU rules: It first of all notes that the extra-territorial application of national law to issues of this kind is not unusual or contrary to public international law, and that national laws of third countries, including the USA, also have extra-territorial effect to activities on the Internet. It gives examples of the extra-territorial (and extra-EU) application of EC rules on competition, consumer protection, commercial agents, and airline passenger data; and of the extra-territorial application of US rules on the online collecting of personal information from children on US territory.[58] One could add the extra-territorial application of US rules on airline passenger data (but should then also note the serious controversy this gave rise to),[59] and of US rules on disclosure of evidence in civil proceedings.[60]

It then goes on to discuss the application of the "applicable law" rules in Article 4 of the Directive to processing of personal data on (or in relation to activities on) the Internet, as follows:[61]

> The situation is different as regards processing operations, which involve a controller in a third country. The national laws of these third countries are not harmonised, the directive is not applicable in these countries and the protection of individuals with regard to the processing of their personal data may therefore be missing or weak. The country of origin principle, which is linked to the establishment of the controller, can no longer serve the purpose of determining the applicable law. It is necessary to switch to another connection factor. The European Parliament and the Council decided to come back to one of the classic connection factors in international law, which is the physical link between the action and a legal system. The EU legislator chose the country of the territorial location of equipment used[62].
>
> The directive therefore applies when the controller is not established on Community territory, but decides to process personal data for specific purposes and makes use of equipment, automated or otherwise, situated on the territory of a Member State.
>
> The objective of this provision in Article 4 paragraph 1 lit. c) of Directive 95/46/EC is that an individual should not be without protection as regards processing taking place within his country, solely because the controller is not established on Community territory. This could be simply, because the controller has, in principle, nothing to do with the Community. But it is also imaginable that controllers locate their establishment outside the EU in order to bypass the application of EU law.
>
> It is worth noting that it is not necessary for the individual to be an EU citizen or to be physically present or resident in the EU. The directive makes no distinction on the basis of nationality or location because it harmonises Member States laws on fundamental rights granted to all human beings irrespective of their nationality. Thus, in the cases that will be discussed below, the individual could be a US national or a Chinese national. In terms of application of EU data protection law, this individual will be protected just as any EU citizen. It is the location of the processing equipment used that counts.
>
> The Community legislator's decision to submit processing that uses equipment located in the EU to its data protection law thus reflects a true concern to protect individuals on its own territory. At international level it is recognised that states can afford such protection.

> Article XIV of the GATS allows to lay down exemptions from the free trade rules in order to protect individuals with regard to their right to privacy and data protection and to enforce this law.

The Working Document goes on to discuss the application of the core terms "establishment", "controller", "equipment", and "making use of equipment", in the context of the Internet.

On the first concept, "establishment", it makes the following observation:[63]

> The place of establishment of a company providing services via an Internet web site is not the place, at which the technology supporting its web site is located or the place at which its web site is accessible, but the place where it pursues its activity.[64] Examples are: a direct marketing company is registered in London and develops its European wide campaigns there. The fact that it uses web servers in Berlin and Paris does not change the fact that it is established in London.

It is notable that this describes a purely intra-EU activity, by an EU-based controller. The result is that, in this example, the controller (the London-based direct marketing company) will be - or at least, in terms of the Directive, ought to be - subject only to the UK Data Protection Act insofar as all its pan-EU personal data processing operations are concerned. It need not bother itself about compliance with the data protection laws in Germany, France, or any of the other EU States in which it conducts campaigns.

But the WP document fails to mention that the situation would not be nearly as easy if the company were to be based in (say) New York. In that case, it would be a controller not established in the EU, who "makes use" of "equipment" in several EU Member States. On that latter point, the WP document has the following to say:[65]

> The determination of when "the controller makes use of equipment for the purpose of processing personal data" in Article 4(1)(c) of the directive is a decisive element for the application of the data protection law in the EU.
>
> The Working Party would advocate a cautious approach to be taken in applying this rule of the data protection directive to concrete cases. Its objective is to ensure that individuals enjoy the protection of national data protection laws and the supervision of data processing by national data protection authorities in those cases where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved.
>
> With this in mind, the Working Party is of the opinion that not any interaction between an Internet user in the EU and a web site based outside the EU leads necessarily to the application of EU data protection law. The Working Party has put forward the view that the equipment should be at the disposal of the controller for the processing of personal data.
>
> At the same time, it is not necessary that the controller exercise full control over the equipment. The extent, to which it is at the disposal of the controller, can vary. The necessary degree of disposal is given if the controller, by determining the way how the equipment works, is making the relevant decisions concerning the substance of the data and the procedure of their processing. In other words, the controller determines, which data are collected, stored, transferred, altered etc., in which way and for which purpose.

> The Working Party considers that the concept of "making use" presupposes two elements: some kind of activity undertaken by the controller and the intention of the controller to process personal data. This implies that not any "use" of "equipment" within the European Union leads to the application of the Directive.
>
> The power of disposal of the controller should, however, not be confused with property or ownership of the equipment, either of the controller or of the individual. In fact, the directive does not attach any relevance to the ownership of any equipment.
>
> The interpretation presented by the Working Party is fully in line with the motivation for the provision in Article 4(1)(c) of the directive given by the EU legislator. Recital 20 explains that "*the fact that the processing is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this directive; whereas in these cases, the processing should be governed by the law of the Member State, in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice".* This is the corollary, which is necessary in order to reach the Directive's broader objective, which is "*to ensure that individuals are not deprived of the protection to which they are entitled under this Directive".*

A little later, the WP discusses, as an example of a situation in which the question of "making use of equipment" arises, the use of "cookies". Leaving aside the technical descriptions, this section concludes as follows: [66]

> As explained above, the user's PC can be viewed as equipment in the sense of Article 4(1)(c) of Directive 95/46/EC. It is located on the territory of a Member State. The controller decided to use this equipment for the purpose of processing personal data and, as it has been explained in the previous paragraphs, several technical operations take place without the control of the data subject. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory.
>
> The Working Party is therefore of the opinion that the national law of the Member State where this user's personal computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk.

The same applies to the use of JavaScript, spyware, etc.: [67]

> Where the controller decides to use these tools [JavaScript] in order to collect and process personal data, he makes use of equipment in the sense of the Directive, and will have to comply with the provisions of EU legislation.
>
> ...
>
> The directive would also apply to information collected through spywares, which are pieces of software secretly installed in the individual's computer, for instance at the occasion of the downloading of bigger software (e.g. a music player software), in order to send back personal information related to the data subject (e.g. the music titles the individual tends to listen to). These kinds of software programs are popularly known as E.T. applications *"because once they have lodged in the user's computer and learned what they want to know, they do what Steven Spielberg's extra-terrestrial did: phone home".* [68]

> This new monitoring software applications often make use of JavaScript and other similar techniques and clearly make use of the equipment of the data subject (computer, browser, hard disc and so on) to collect data and send it back to another location.
>
> (NB: The WP document goes on to say that: "As these technologies are by definition used without informing the user (the name spyware is clear in that respect) they are a form of invisible and not legitimate processing." But that is a separate point and does not affect the question of applicable law.)

These may well be the correct interpretations of the words "equipment" and "making use of equipment"; they are certainly in line with the apparent intention of the European legislator, as the WP points out. However, the application of this approach to non-EU based controllers is still highly problematic, even with the *caveats* entered by the WP about the need to be "cautious". This can be shown easily if we apply the proposed approach to the example given by the WP for purely intra-EU marketing, but with the controller placed this time outside the EU, e.g., as already suggested, in New York.

First of all, in this case that controller undoubtedly "makes use" of "equipment" in Germany and France, because it uses web-servers there. But if its activities include sending "cookies" to visitors to its website(s) from other EU Member States, and/or using JavaScript to collect data on them, the New York company would also, in this view, be "using equipment" (i.e., the PCs of its visitors) in those other States. *And each of those States should, under Article 4(1)(c), apply its law in full to the New York company's personal data processing activities*. A US-based company wishing to carry out a pan-European (pan-EU) campaign, from New York, involving the sending of "cookies", must therefore, under the rules in the Directive, simultaneously comply with no less than 27 (or even, with the EEA countries, 30) (!) different national data protection laws (and as we shall see below, at (b), these still vary considerably in their detail).

There is one *caveat* that may bring non-EU-based controllers some relief. This is the comment of the WP, already quoted, that:[69]

> the concept of "making use" presupposes two elements: some kind of activity undertaken by the controller and the intention of the controller to process personal data. This implies that not any "use" of "equipment" within the European Union leads to the application of the Directive.

Presumably, this means that if there is no specific *intention* to target EU-based individuals, the rules of the Directive need perhaps not apply (or be applied in practice by the national DPAs). But this is a very difficult line to draw. If a US-based company has a website that is really aimed only at US consumers, it might, under this approach, escape the EU rules. However, if it were to send "cookies" from this website to all its visitors, including EU-based individuals, this would become more doubtful. If it were to use these "cookies" to identify EU-based visitors, and then sends them (but not its US-based visitors) a special message - perhaps informing them of its EU-based sister company and its website - then it could be said no longer to escape this exemption. If it were to sell EU citizens goods and services directly online, as part of its global offers, it would almost certainly come within the scope of the EU laws. There is moreover no procedure to ensure that this *caveat* is applied in practice by all the EU DPAs, or that, if it is applied, it is done so in a consistent manner.

(b) Applying The "Appliable Law" Rules In National Laws To The Internet

Similar to the situation at EU 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 Internet, 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 Internet. 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." In principle, their own domestic data protection law therefore applies to these 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. We will discuss some of the guidance given in this respect later, in Part 4.

In spite of some ambiguities, the data protection authorities in the EU Member States generally also do not seek to apply their national laws to Internet operations by controllers established in other EU Member States - at least not as long as they feel reasonably confident that the citizens of their country are more or less adequately protected by the data protection law in that other EU State. They do not even do so if their national law, contrary to the Directive, clearly suggests that the law ought to apply, or can be interpreted in that way. Indeed, the formal requirements which some laws impose - such as the requirement in the Greek law that all non-Greek controllers who collect data on Greek citizens must appoint a representative in Greece, even if they are based in another EU Member State - are also apparently not enforced in practice (although in such respects, the law should still be amended to remove such ideosyncracies, as is now apparently being done).

Few if any problems have therefore arisen in this respect in practice to date. However, this could change in the new global technical environment described in Working Paper No. 1, especially in respect of non-professional users of the Internet, more in particular if the exemptions for "purely personal processing" and freedom of expression, discussed in section 2 were to be differently applied in this context. Thus, as already mentioned there, it would be difficult for some countries to accept that personal data on their citizens would be left unprotected under the "applicable" law of another Member State, because that other Member State were to hold that the individuals who uploaded the data to the "cloud" (from where they are accessible in the first Member State) benefitted from the "purely personal processing" exemption, if that exemption were not to be applicable in the first State. Conversely, it would be unacceptable to some countries if the dissemination of information by some of their citizens, which under their own law would be regarded as covered by the "freedom of expression" exemption, and thus allowed, were to be held to be illegal under the data protection law of another Member State, if that latter State were to claim that its law was "applicable", and if that State did not apply that exemption in the case (or not as generously as the first State).

There is also the complication (also already mentioned), that unlike companies and organisations, which are usually quite clearly "established" in a given place and State,

individuals who provide user-generated content can, and do, freely move. They can upload data from one country one day, and from another the next. It is quite unclear how the EU Member States regard such individuals in terms of their law: the usual *nexus* is the place of "establishment" of the controller. Does that mean, for private citizens, their place of usual residence? If so, what happens to the information they have uploaded to the Web, when they change residence? Should they review if they have suddenly become subject to the data protection law of their new place of residence in respect of their materials in the "cloud"? If under the law of their previous place of residence they did not need the consent of certain data subjects because they benefitted from an exemption, should they now retrospectively seek it, if in their new home country that exemption, under the law of that country, no longer applies?

These scenarios may seem complex, and may still be rare, but in the new environment they are far from hypothetical. On the contrary, in the "Web 2.0" environment, in which most of the material on the Internet is user-generated, such cases would be common. The EU will need to clarify the law in this respect, and this should include the difficult task of harmonising the scope and practical application of the "purely private processing" and "freedom of expression" exemptions.

A further intra-EU problem, also already noted, concerns the First Pillar – Third Pillar dichotomy. At the moment, there is still only relatively limited activity by the law enforcement and security agencies on the Internet, but this quickly changing. Yet as noted in section 2.1, several Member States have uncritically extended the "applicable law" rules, and the principle of unimpeded transfers within the EU - which of course are fundamental to the Directive - to issues not covered by the Directive, in the Third Pillar. This means that, under those law (and unless there are other laws that stand in the way), personal data can be freely transferred over the Internet from such countries to any other EU Member State, for law enforcement or national security purposes - even if the recipient EU country has no, or no adequate, data protection rules that apply to such processing at all.

It also sometimes means that, at least on paper, activities of law enforcement agencies of other EU Member States that directly target individuals in the first Member States (such as remote surveillance, or even "hacking" [on-line searching"] of their PCs), are not subject to the data protection laws of the EU Member States where the targets of such actions live, but only to the domestic laws of those foreign agencies - which in this respect may well be seriously defective from the perspective of the State whose citizens are the subject of such activities (and even more so from the perspective of those citizens!).

These are far from trivial matters. They have the potential to seriously undermine the data protection system within the EU, and the faith of citizens in it, and must be addressed in the face of the new environment - in which, of course, now that the Lisbon Treaty has come into force, the "pillars" are in any case abolished. It strongly underlines the need for a single EU data protection regime across all the now-abolished three pillar areas (albeit of course subject to appropriate special rules and exemptions for law enforcement and national security matters).

The main problems arise, however, in respect of the activities of non-EU controllers on the Internet. It is clear that many - although not all - Member States are reluctant to regard such activities as beyond the scope of their national data protection law, when they can often

directly affect (the data of/on) their citizens. The simplest way to ensure the application of their laws is to take a broad view of what constitutes "means" or "equipment" used to process personal data. It is clear that most of the data protection authorities in the EU regard the use of "cookies" and JavaScript to collect data on their citizens, as sufficient to bring the processing of the data by a non-EU controller within the scope of their laws. As we have seen, they have also collectively taken that view, in the Article 29 Working Party.

This is in principle fully understandable: from a European perspective, data protection is an important fundamental right - and becoming more so in the new global technical environment - and European citizens should therefore not be robbed of such protection just because they visit websites of non-EU controllers. This is of course all the more so since the Web is still dominated by US-based companies, and the laws in the USA provide much less protection than the European laws (as shown in the Country Report on the USA).

The problem here therefore lies not so much with the principle, as with the way the Directive and the national laws apply, once one takes such a broad view of these concepts.

In particular, as we have seen, the rules in the Directive, as applied in the national laws of the Member States, result in the untenable situation in which non-EU-based controllers with an Internet presence throughout the EU - which includes all the most important players on the Internet - are simulataneously subject to the laws of every single EU Member State (plus the EEA States, plus the laws of candidate States and of other States that follow the Directive), and should appoint a representative in each of these States who will be held responsible for compliance, by the non-EU controller, with the law in the country where he has been appointed, "without prejudice to legal actions which could be initiated against the controller himself", as the Directive so simply puts it (Article 4(2)).

In fact, these requirements are not even, formally, affected if a US-based controller of this kind were to join the "Safe Harbor": that would provide a presumption that the controller provides "adequate" data protection, and that data can thus be transferred to the controller in the USA - but it does not guarantee full compliance with every applicable provision of every applicable law.

This is a most serious issue in a globalising world, that must be given serious attention.

4. The difficulties in determining *how*, if applicable, EU data protection law should be applied in the new technical global environment

This section examines the (often quite varying) ways in which specific concepts, principles, criteria, rules and requirements of the main data protection directive have been transposed into the data protection laws of the EU Member States, and notes both the general difficulties with some of these concepts, rules and requirements in the new global-technical environment described in Working Paper No. 1, and the problems that arise because of the divergent transpositions. The two are linked, in that divergent transpositions further complicate the general difficulties, especially in relation to the kinds of transnational/global operations that are increasingly common in that new environment (indeed, that are an inherent aspect of that environment).

We will look first at a number of core concepts, at the definitions in the Directive and in the national laws and at the way these are applied in practice. Next, we will look at the main data protection principles and the criteria for lawful processing, including their application in relation to processing of sensitive data and to processing for (in the Directive, not further defined) "substantial public interests". We will then look at data subject rights and the limitations on and exceptions to those rights. In the final two sub-sections, we will examine the rules in the Directive and the national laws relating to data security, and to transborder data flows. For reasons of space, the analyses in this section have had to be kept short, often by paraphrasing information provided in more detail elsewhere.[70] As before, we will end this section with some tentative, provisional comments.

4.1 CORE CONCEPTS AND DEFINITIONS

In this sub-section, we will look at the following concepts:

- "personal data" and "data subject", in particular in relation to:
  - the general elements of the definitions, including the questions of how IP addresses "relate" to individuals, and of identifiability of data generally;
  - the more specific question of anonymisation, pseudonymisation and re-identifiability; and
  - the special issue of "profiling" as it arises in this context;
- "processing [of personal data]";
- "controller" and "processor".

In each case, we will again focus on the problems that perhaps already arise in the present context, but that are, or will become, particular pressing in the new global-technical environment described in Working Paper No. 1.

"PERSONAL DATA" AND "DATA SUBJECT", AND THE ISSUES OF ANONYMISATION, PSEUDONYMISATION, RE-IDENTIFIABILITY AND "PROFILING":

(a) The Concepts of "Personal Data" And "Data Subject", And The Issues of Anonymisation, Pseudonymisation, Re-Identifiability And "Profiling", In The Directive:

The concepts of "personal data" and "data subject" are central to the application of the Directive and the national laws that implement the Directive. In the Directive, the two concepts are closely linked, and defined in the same paragraph, Article 2(a), as follows:

> '**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;

The Article 29 Working Party has issued a very important Opinion on this concept.[71] The Introduction to this Opinion itself makes its direct importance to the present study very clear: [72]

> The Working Party is aware of the need to conduct a deep analysis of the concept of personal data. Information about current practice in EU Member States suggests that there is some uncertainty and some diversity in practice among Member States as to important aspects of this concept which may affect the proper functioning of the existing data protection framework in different contexts. The outcome of this analysis of a central element for the application and interpretation of data protection rules is bound to have a profound impact on a number of important issues, and will be particularly relevant for topics such as Identity Management in the context of e-Government and e-Health, as well as in the RFID context.
>
> The objective of the present opinion of the Working Party is to come to a common understanding of the concept of personal data, the situations in which national data protection legislation should be applied, and the way it should be applied. Working on a common definition of the notion of personal data is tantamount to defining what falls inside or outside the scope of data protection rules. A corollary of this work is to provide guidance on the way national data protection rules should be applied to certain categories of situations occurring Europe-wide, thus contributing to the uniform application of such norms, which is a core function of the Article 29 Working Party.

Apart from noting the general importance of clarification of the concept of personal data, this quote also touches on the importance of a more uniform application of the Directive generally, and on the important role the Working Party plays, or can play, in this regard. We will return to that in our Final Report.

More specifically, the Opinion analyses the various elements in the definition: "any information", "relating to", "identifiable" and "natural person"; and it also comments on what happens if data fall outside the definition.

Below, we very briefly summarise the comments of the Working Party in respect of the first three of the above-mentioned elements in the definition, as far as possible in the very words used by the Working Party, with emphasis - and some further brief comments - on matters of particular concern to the present study. On the question of the limitation of the concepts of "personal data" and "data subject" to (data on) "natural persons", it will suffice in the present context to note that this means that the Directive only applies to living human beings, but that the Member States are allowed to extend their national laws beyond that[73] (some borderline cases, raising the question of whether certain data on legal persons such as companies may also, at times, constitute personal data in the sense of data on "natural persons" will however be noted in the sub-sections below).

As concerns the question of data outside the scope of the definition, it may suffice to mention that the Working Party rightly notes (with reference also to the *Linqvist* judgment of the ECJ, already mentioned) that States are allowed to apply their national data protection laws more broadly than the Directive, and can therefore include data that are not covered by the latter; and that in any case: [74]

> Where data protection rules do not apply, [the collecting and further processing of information about] certain activities may still constitute an interference with Article 8 of the European Convention on Human Rights, which protects the right to private and family life, [or may be subject to other] sets of rules, such as torts law, criminal law or antidiscrimination law.

After the discussion of the three main elements of the definition, below, we will briefly discuss the two specific issues listed above: "anonymisation, pseudonymisation and re-identifiability", and "profiling".

"*any information*":

The Working Party rightly stresses that it follows from the fact that the Directive is a human rights instrument, that the concept of "personal data" must be widely interpreted. It is emphatically not limited to information touching the individual's private and family life "*stricto sensu*", or to information of a particularly intrusive, private nature. Mundane, trivial, even publicly-available information, is all included (such information may be subject to relatively lax rules, but that is another matter).[75]

Subject to the "purely private or household" and "freedom of expression" exemptions discussed in section 2.2, it includes information on individuals, regardless of the position or capacity of those persons (as consumer, patient, employee, customer, etc), and relating to their private, public, recreational and work activities.

It also includes information available in whatever form, be it alphabetical, numerical, graphical, photographical or acoustic. It includes information kept on paper, as well as, e.g., information stored in a computer memory by means of binary code, or on a videotape. The Directive explicitly confirms that "sound and image data" are "personal data" if they relate to an identifiable individual (see Recital 14); data from closed circuit television (CCTV) cameras, videoconference- or just -calling systems or "webcams", are thus all, in principle, included (even if, for now, most CCTV systems are still incapable of effective face-recognition:[76] that will rapidly change in the near future).

It is not necessary for the information to be considered as personal data that it is contained in a structured database or file; even if it is unstructured, if it is processed by automated means (read: by computer, or over the Internet), it comes within the scope of the Directive. Information contained in free text in an electronic document or webform - or indeed in an email or SMS message ("text"), or in an attachment to such messages, e.g., an instantly-sent photograph or videoclip - will therefore qualify as personal data, if the other criteria in the definition of personal data ("relating to", "identifiable" and "natural person") are fulfilled. Almost needless to say, in the new global-technical environment, the creation and (worldwide transnational!) dissemination (= processing) of such data is expanding at an explosive rate. Photographs and videos furthermore often "reveal" sensitive data: race of course, but also religion (by showing certain symbols, or by the context, such as a church wedding), physical disabilities, or sexual inclination: see sub-section 4.4, below.

The concept of personal data moreover includes not just factual records (name, date of birth, address, occupation, bank account number, etc.) but also opinions, intentions and predictions

in relation to an individual ("John is a hard worker"; "Sandra is not suitable for promotion to area manager"; "Jimmy is likely to grow up to become a criminal"; etc.).

Data can be "personal" in respect of more than one person. A prescription, for instance, can be "personal" in relation to both the patient and the doctor writing it (and indeed, the pharmacists who provides the medicine). Emails (or separate parts of an email), too, can be "personal" in relation to different persons: the sender, the recipient(s), and anyone mentioned in the email (or to whom it otherwise relates). Photographs can of course also show several persons, and indeed suggest certain relations between them.

Special mention must be made of biometric data, the use of which will strongly increase in the new global-technical environment. On this, the Working Party has the following to say:[77]

> [Biometric data] may be defined as biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability. Typical examples of such biometric data are provided by fingerprints, retinal patterns, facial structure, voices, but also hand geometry, vein patterns or even some deeply ingrained skill or other behavioural characteristic (such as handwritten signature, keystrokes, particular way to walk or to speak, etc...)
>
> A particularity of biometric data is that they can be considered both as *content* of the information about a particular individual (Titius has these fingerprints) as well as an element to establish a *link* between one piece of information and the individual (this object has been touched by someone with these fingerprints and these fingerprints correspond to Titius; therefore this object has been touched by Titius). As such, they can work as "identifiers". Indeed, because of their unique link to a specific individual, biometric data may be used to identify the individual. This dual character appears also in the case of DNA data, providing information about the human body and allowing unambiguous and unique identification of a person.
>
> Human tissue samples (like a blood sample) are themselves sources out of which biometric data are extracted, but they are not biometric data themselves (as for instance a pattern for fingerprints is biometric data, but the finger itself is not). Therefore the extraction of information from the samples is collection of personal data, to which the rules of the Directive apply. The collection, storage and use of tissue samples themselves may be subject to separate sets of rules.[78]

"*relating to*" *[an identified individual]*:

According to the Working Party, there are several ways in which data can be said to "relate" to an individual: "*In order to consider that the data "relate" to an individual, a 'content' element OR a 'purpose' element OR a 'result' element should be present.*" [79] It goes on to clarify this as follows (with small editorial changes):[80]

The "content" element is present in those cases where - corresponding to the most obvious and common understanding in a society of the word "relate" - information is given about a particular person, regardless of any purpose on the side of the data controller or of a third party, or the impact of that information on the data subject. Information "relates" to a person when it is "about" that person, and this has to be assessed in the light of all circumstances

surrounding the case. For example, the results of medical analysis clearly relate to the patient, or the information contained in a company's folder under the name of a certain client clearly relates to him. Or the information contained in an RFID tag or a bar code incorporated in an identity document of a certain individual relates to that person, as in future passports with an RFID chip.

In some situations, the information conveyed by the data concerns objects in the first instance, and not individuals. Those objects usually belong to someone, or may be subject to particular influence by or upon individuals or may maintain some sort of physical or geographical vicinity with individuals or with other objects. It is then only indirectly that it can be considered that the information relates to those individuals or those objects. Thus, the value of a house in a particular area may not constitute personal data in the general context of a discussion of house prices in a region, but it will constitute personal data if it is linked to, say, the tax liability of an identified individual (typically, the house owner).

We may add that this is a likely growth area in the new global technological environment: in that environment, there will be increasing (indeed, exponentially increasing) amounts of such "closely-but-perhaps-not-fully" person-related data. In an era of ubiquitous computing, "things" associated with individuals - from cars to PCs to printers to fridges to 'phones to payment cards to Internet user IDs - will increasingly leave traces: they provide a record of where the car or the 'phone was, what websites were visited by the user of the PC, of whether, and when, the printer automatically ordered a new toner cartridge, or the fridge milk; they leave a trace of when a card (perhaps an anonymous card) was used to make a certain payment, or whether a particular Internet ID was used to access a particular website. There is no conclusive link with the owner of the car or the PC or the 'phone, or the printer or the fridge, or even the original buyer of the card or the person who obtained the ID. Some of these matters (anonymous payment cards, certain Internet IDs) may indeed have been established with the very aim of distancing the "real" person from the recorded matter (for good or bad reasons); sometimes, someone linked to or using the "thing" may have pretended to be someone else (possibly through what is wrongly called "identity theft"). Yet more often than not, the data will relate, or at least probably relate, to a specific individual.

The general approach of the Working Party in this respect is clear: if anything, it feels it (and the national DPAs) should err on the side of applying the law, rather than ruling that data, in terms of "content", are not sufficiently "related" to an individual to constitute "personal data", and that the law therefore does not apply. This is clear, e.g., from the Working Party's approach to the question of how to treat IP addresses. In that context, the Working Party says that:[81]

> unless [an] Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side.

The same applies to "traffic data" and "location data", as defined in Article 2, paras. (b) and (c), of the e-Privacy Directive (Directive 2002/58/EC):

> (b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

> (c) loccation data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

As such, these data clearly relate to "things": to the data needed to send messages from one "thing" to another, and to locate the "thing" used to send the messages. However, they are of course closely related to the user, and reveal much about the user: with whom he or she communicates, for how long and how often, and perhaps whether there is a pattern of communications (with A systematically calling B after being called by C, etc.). Given the Working Party's views on IP addresses, just noted, it is not surprising that they regard communication traffic and location data as equally, in principle, constituting "personal data", whenever those data are in one way or another linked to (the equipment of) a particular user. This is if anything reinforced by the application of the other criteria, "purpose" and "result", which we will discuss now.

According to the Working Party, a "purpose" element, too, can be responsible for the fact that information "relates" to a certain person. That "purpose" element can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual. Thus, when a company keeps logs of IP addresses with a view to identifying Internet users who illegally download copyright-protected material, those logs *ipso facto* contain personal data, even if not all the IP addresses are instantaneously - or even at all - linked to specific PCs and specific PC users. The very fact that the purpose of the record-keeping is the identification of (some, still-to-be-identified) individuals, is enough to bring all of the records within the scope of the law. [82]

Finally, a third kind of "relating" to specific persons arises when a "result" element is present. According to the Working Party, despite the absence of a "content" or "purpose" element, data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case. It should be noted that it is not necessary that the potential result be a major impact. It is sufficient if the individual may be treated differently from other persons as a result of the processing of such data. The Opinion gives the following example, of monitoring of the GPS position of taxis, with the aim to optimise the service to clients, but which has a clear impact also on the taxi drivers: [83]

> A system of satellite location is set up by a taxi company which makes it possible to determine the position of available taxis in real time. The purpose of the processing is to provide better service and save fuel, by assigning to each client ordering a cab the car that is closest to the client's address. Strictly speaking the data needed for that system is data relating to cars, not about the drivers. The purpose of the processing is not to evaluate the performance of taxi drivers, for instance through the optimization of their itineraries. Yet, the system does allow monitoring the performance of taxi drivers and checking whether they respect speed limits, seek appropriate itineraries, are at the steering wheel or are resting outside, etc. It can therefore have a considerable impact on these individuals, and as such the data may be considered to also relate to natural persons. The processing should be subject to data protection rules.

Several of the criteria just discussed (including the latter one, of the "result" [or effect] of the processing) are especially relevant (also) to the question of "profiling", as discussed under a

separate sub-heading, below. First, however, we will discuss the final main element in the definition: identifiability.

"*identifiable*":

The Working Party Opinion is quite detailed on the various aspects of this element,[84] but its basic approach can be relatively simply summarised: The main point about identification of a person is not whether one knows the name of the person, but rather, whether the person can be distinguished from other members of the group within which he or she is placed or found (e.g., from within a database or other data collection). Or, we may add, whether one can link information on an otherwise unknown person to information held elsewhere, as when one can determine that a person in one CCTV image is the same person as is captured in another such image (or in a database of, say, suspected shoplifters).

In the new global technical environment described in Working Paper No. 1, there are new ambiguities in this regard: increasingly, there will be what we may call temporary (quasi?-) identification. Thus, for instance, in a supermarket's computer system trolleys (rather than shoppers) may be "tagged", and identify the items placed in the trolley. "The system" may then make an offer to the shopper using a particular trolley, e.g., an offer of a free packet of washing powder, to try that powder out. The offer will be based on the record of the other items in the trolley; it is not based on any personal characteristic of the shopper (other than that that shopper is in charge of that trolley). On the other hand, the offer is specifically made to *this* shopper (and others selected by the system on the basis of some algorithm), not to all shoppers. The question arises whether the shopper is "identified" by the system, and "identifiable" to the supermarket.[85] Presumably, the answer is in the affirmative.

In the London Underground, pictures from CCTV cameras are automatically analysed, by a computer that can detect behaviour patterns that may indicate that a particular person intends to commit suicide by throwing himself before an oncoming train. On the one hand, the system, by its very nature, collects information on everyone (and presumably retains this for a limited time), but it singles out only a very few for individualised attention (a security person is sent to the platform in case of an alert). On the basis of the Working Party's approach, one must conclude that the person causing the alert is "identified" - not by name, but by being distinguished from the ordinary, non-suicidal travellers.

As the very text of Article 2(a) of the Directive makes clear, the issue is not whether the person *is* actually identified (by the controller, or indeed someone else), but whether he or she is *can be* identified (by the controller or someone else).

This latter question depends in part on the existence of, and access by different people or organisations to, various full or partial "identifiers": data which (in the sense discussed earlier) "relate" to a person. As the Working Party puts it:[86]

> the extent to which certain identifiers are sufficient to achieve identification is something dependent on the context of the particular situation. A very common family name will not be sufficient to identify someone - i.e. to single someone out - from the whole of a country's population, while it is likely to achieve identification of a pupil in a classroom. Even ancillary information, such as "the man wearing a black suit" may identify someone out of the passers-by standing at a traffic light. **So, the question of whether the**

> **individual to whom the information relates is identified or not depends on the circumstances of the case.**

Crucially, the Directive applies whenever an individual is identified or identifiable "directly or indirectly"; and the latter includes circumstances in which someone or some body (public or private), who may or may not be the controller, is capable of achieving this: [87]

> As regards "indirectly" identified or identifiable persons, this category typically relates to the phenomenon of "unique combinations", whether small or large in size. In cases where *prima facie* the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information (**whether the latter is retained by the data controller or not**) will allow the individual to be distinguished from others. ...

The Working Party adds that: [88]

> Some characteristics are so unique that someone can be identified with no effort ("present Prime Minister of Spain"), but [as concerns others] a combination of details on categorical level (age category, regional origin, etc) may also be pretty conclusive in some circumstances, particularly if one has access to additional information of some sort.

The Working Party points out that Recital 26 of the Directive pays particular attention to the term "identifiable" when it says that "[*in order*] *to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.*" It explains that this means that a mere hypothetical possibility to single out the individual is not enough to consider the person as "identifiable". If, taking into account "*all the means likely reasonably to be used by the controller or any other person*", that possibility does not exist or is negligible, the person should not be considered as "identifiable", and the information would not be considered as "personal data". The criterion of *"all the means likely reasonably to be used either by the controller or by any other person*" should in particular take into account all the factors at stake. The cost of conducting identification is one factor, but not the only one. The intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organisational dysfunctions (e.g. breaches of confidentiality duties) and technical failures should all be taken into account.

It then adds an important comment, saying that:

> On the other hand, this test is a dynamic one and should consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed. Identification may not be possible today with all the means likely reasonably to be used today. If the data are intended to be stored for one month, identification may not be anticipated to be possible during the "lifetime" of the information, and they should not be considered as personal data.
>
> However, it they are intended to be kept for 10 years, the controller should consider the possibility of identification that may occur also in the ninth year of their lifetime, and which may make them personal data at that moment.

Other matters to be considered are the means used in the processing of the data, and the purpose(s) of the processing:

> One relevant factor, as mentioned before, for assessing "*all the means likely reasonably to be used*" to identify the persons will in fact be the purpose pursued by the data controller in the data processing. National Data Protection Authorities have been confronted with cases where, on the one hand, the controller argues that only scattered pieces of information are processed, without reference to a name or any other direct identifiers, and advocates that the data should not be considered as personal data and not be subject to the data protection rules. On the other hand, the processing of that information only makes sense if it allows identification of specific individuals and treatment of them in a certain way. In these cases, where the purpose of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved have or will have the means "likely reasonably to be used" to identify the data subject. In fact, to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms. Therefore, the information should be considered as relating to identifiable individuals and the processing should be subject to data protection rules.

The Working Party concludes on the above basis that, for instance, video surveillance which is aimed at identifying certain persons (like shoplifters), *ipso facto* involves processing of "identifiable" data, even if most of the video images captured will never be related to specific individuals. Similarly, as already noted, it feels that if certain entities keep - or seek to obtain - logs of IP addresses, with the specific aim of identifying those which they feel are linked to illegal activity such as copyright infringement, those entities will automatically be processing identifiable personal information - again, even if in many, even most instances, they will not link the IP addresses to a particular PC or person.[89]

In our view, all the above consideration are eminently sensible from the point of view of the Directive and of data protection as a fundamental right. However, it should be noted that, in the light of the information in Working Paper No. 1 about the developments in data dissemination, in the capabilities of data processing and –matching, and in the vastly expanding access to (by current standards) highest-level capabilities of data processing and –matching, by pretty much anyone, the application of the above thinking will mean that enormous amounts of information that are currently considered (or that until recently would have been considered) "non-identifiabe" are becoming "identifiable" - and hence "personal", and hence subject to European data protection law. This applies in particular to vast amounts of disparate information that can be found on the Internet.

In the new global technical environment, individuals, but perhaps more importantly (and dangerously) State bodies and corporate agencies, can trawl through endless amounts of such disperate data and, using sophisticated technologies, can link up CCTV images, "YouTube" clips, blogs and other supposedly unrelated data items, on individuals who may never have been aware that their data (their images, or seemingly private interactions) could thus be matched - and indeed, could thus be collated by total strangers, and unknown entities.

The clear implication of the approach taken by the Working Party is that, subject to the application of the exemptions and "applicable law" rules discussed in Parts 2 and 3, above, anyone, and any body (public or private), that engages in such "trawling" and "data

matching" exercises, is - indeed must be - subject to the European data protection law and – principles.

We do not disagree with this view. However, as we have seen, those "applicable law" rules are difficult enough to comply with in respect of purely intra-EU processing, but can be very onerous if applied to global activities, especially on the Internet. We feel that the implications of the Working Party's approach in this global context have not yet been fully thought through. We will return to this in our Final Report. Indeed, in that context, we will also take account of the next, related issue: the question of anonymisation, pseudonymisation and the problem of re-identifiability.

"*anonymisation, pseudonymisation and re-identifiability*":

In its Opinion on personal data, the Working Party also addresses, to some extent, the question of anonymisation and pseudonymisation of data. These matters are seen as part of the issue of "identifiability": "anonymous" data are data that cannot be linked to a specific individual; "anonymised" data are data that once were linked to such an individual but that can now no longer be related to that person; and "pseudonymised" data are data that can only be linked to such a person if one has possession of a decoding "key". Thus, the subject of "anonymous" data is not identifiable; the subject of "anonymised" data is no longer identifiable; and the subject of "pseudonymised" data is only indirectly identifiable, by means of the "key".

There are two sets of problems with this. First of all, even on its own terms, the Working Party's Opinion shows that these categories are not as absolute, or clearly delineated, as it seems, and that the practices aimed at anonymisation of pseudonymisation described in the Opinion are not as effective as one might think - and will become less so in the new global technical environment described in Working Paper No. 1. We will show this below.

However, secondly, we should also point out that, according to leading experts in this field, the Working Party's whole understanding of the issues is deficient: the Working Party (as we shall see) seems to believe that pseudonymisation or anonymisation depend on the quality and effectiveness of the measures used, and in particular on the level of encryption. However, in reality they depend on the size of the data sets involved. We will briefly return to this fundamental issue at the end of this sub-section, but will deal with this in fuller detail in our Final Report. For now, we will follow the Working Party's lines of reasoning.

Thus, the Working Party believes that pseudonymisation by means of one-way cryptography "creates *in general* anonymised data", subject to the *caveat* that the effectiveness of the pseudonymisation procedure depends on a number of factors: at which stage it is used, how secure it is against reverse tracing, the size of the population in which the individual is concealed, the ability to link individual transactions or records to the same person, etc..[90] Elsewhere, the Opinion mentions as other factors to take into account: the risks of an external hack, the likelihood that someone within the sender's organization - despite his professional secrecy - would provide the key. and the feasibility (= statistical probablity? DK) of indirect identification.[91]

The general approach of the Working Party is clear from various examples it gives.[92] This includes medical clinical trials, in which a company instructs a researcher to key-encode (= pseudonymise) patient-identifiable data (so that if needs be the patients can be warned of adverse effects of the medicine being tried), but with only encoded data being passed on to third parties (or released in publications). The Opinion is not entirely explicit, but suggests that for the researcher the data are obviously identifiable and personal; and that the company, being the controller of the processing, should therefore also, in respect of all the processing, be regarded as processing "personal data" and thus as subject to the law; but that third-party recipients *may* be regarded as not receiving personal (i.e., identifiable) data, provided: (i) the relevant protocols and procedures were explicitly designed with a view to excluding re-identification (and thus, for instance, explicitly forbade third-party recipients from trying to re-identify the data), and (ii) "appropriate technical measures (e.g., cryptographic, irreversible hashing)" have been put into place to prevent re-identification.

Even then, the Opinion recognises that re-identification may still occur "due to unforeseeable circumstances such as accidental matching of qualities of the data subject that reveal his/her identity". However, this is not because of any "means likely reasonably to be used" by the original controller, or which that controller could reasonably expect the recipient/new controller to use; it is just pure chance. The Opinion does not address the much more realistic scenario, discussed at the end of this sub-section, of an "attacker" using statistical search methods to identify a person on whom the attacker has anonymised data, by matching it with other data.

In a case of re-identification purely by chance, the Opinion suggests, the data were not "personal data" when they were disclosed, and the disclosing organisation was therefore not subject to the law in that respect. The recipient also, initially, did not receive personal data, and was therefore also not subject to the law in relation to the encoded data. However, once the new controller did (accidentally) gain access to the identity of the data subjects, the thus re-identified data "will undoubtedly be considered to be 'personal data'", and the processing of those data will thus become subject to the law. [93]

The application of the law on this basis would thus appear to depend on two matters:

- the soundness of what Article 17 of the Directive calls the "technical and organizational measures" adopted by the controller, including anything from chosing trustworthy staff and training them appropriately, through proper rules, protocols and procedures (including logs, etc.), to "appropriate" (= "state of the art") technical measures, such as encryption and encoding; and

- the probability of accidental re-identification of the data, in spite of the above measures.

The two are linked, in that the measures mentioned in the first bullet-point are to be aimed at minimising the probability mentioned in the second - although it is recognised that that probability can never be reduced to zero. Particularly important in the assessment are the "means likely reasonably to be used" by anyone who is given (or who may foreseeably obtain) access to the encoded data.

We may note that, even if one takes the above analysis by the Working Party at face value, anonymity of data will be much more difficult to maintain in the new global-technical

environment described in Working Paper No. 1, if only because highly sophisticated "data matching" software will be much more readily available, to law enforcement agencies and other public bodies, but also to companies and private individuals. Some types of data, which until recently could not be easily linked to other data, such as photographs or videoclips, can increasingly be so linked, in the latter case through face-recognition software that can "trawl" through the Internet looking for matches of a picture of an individual. Even in the rather basic scenario underpinning the Working Party's analysis, anonymity will become much harder to achieve.

In fact, the situation is more problematic. This is because re-identifiability of anonymised or pseudonymised data does not require the compromise of the "key": the questions of sophisticated encryption and "purely by chance" re-identification are largely red herrings. Rather, as already mentioned, data security, including privacy-security in the sense of data not being "identifiable", depends on the size of the relevant data set. As one of our special advisers, Professor Ross Anderson of Cambridge University, put it:[94]

> the relevant measure is the size of the anonymity set - that is, the set of individuals to whom a sensitive datum might pertain. If you're described as "a man" the anonymity set size is three billion [half the world's population - DK], while if you're described as "a middle-aged Dutchman with a beard" it's maybe half a million and if you're described as "a middle-aged Dutchman with a beard who lives near Cambridge" it might be 3 or 4.
>
> The size of anonymity set you need depends on the application. If you want to avoid a criminal conviction, two is enough [because unless a court can determine which of the two is the criminal and which the innocent, both will go free – DK]; but that won't do if the fear is stigmatisation, or going on the "no-fly list" [because you are deemed to be a probable terrorist - DK].
>
> The problem with pseudonyms is that if they're used for more than one purpose, the anonymity they give rapidly erodes, and this is the case regardless of the form of the pseudonym itself [and indeed, irrespective of whether, or how well, the pseudonym is encrypted - DK]. Suppose we gave everyone in the world an ID card with a secret number and you were human no. 3,265,679.016; that's functionally the same as a longer "cryptographically secure" number such as 2a45 380f 4513 3da2 8770 fa21 a237 3cb1 because if the opponent knows it refers to a human, the anonymity set size is the same.
>
> Regardless of whether you use long or short numbers, how such systems break is this. You first pseudonymise a single incident, such as a drug prescription: "human no. 3,265,679.016 got penicillin on 3/2/09". The anonymity set size just shrunk from six billion to a few hundred thousand. Then along comes a second incident: "human no. 3,265,679.016 got codeine on 14/5/09". Now it's down to a few hundred or even a few dozen. A couple more incidents and you're uniquely specified.

In other words, it is effectively impossible to keep data truly unidentifiable once the basic information is released, even in encoded form, if there are other data sets against which the pseudonymised or anonymised data can be matched: by matching elements in the released (and supposedly unidentifiable) data ("Dutch", "male", "beard", "near Cambridge", etc.) against the same elements in various other data sets, the "target" can usually be quickly narrowed down to just a very few people, or indeed to the one single data subject.

It is against this fact that we must assess the effectiveness of anonymity, pseudonymity and encoding in the new global-technical environment. In that environment, ever-increasing amounts of information will be ever-more routinely released over the Internet. Some of it will be in structured form: population data or electoral rolls, land registers, registers or directories of shareholders, company directors, staff directories, lists of names of people who in their youth attended a particular school or university, census data, credit reference files, etc.. Some of it may be unstructured: text and photographs and videoclips on SNS sites, etc. Some of these data may in theory be restricted, or even legally confidential, but they are often barely protected. Any halfway determined (and technically aware) person can use such other data sets to try and re-identify supposedly fully-anonymised or pseudonymised data, without any need for the "key".[95]

We will return to this issue in our Final Report.

"*profiling*":[96]

A "profile", in the sense in which that term is used in data processing, is a means to identify a particular, pre-specified kind or type of individuals. In the past, profiles have been very basic: e.g., men between the ages of 20 and 25 with a disposable income of more than (say) twenty thousand euros per annum could be regarded as "typical" readers of a particular magazine; or women who buy certain make-up products, as "typical" customers of a particular kind of shop, etc. Old-fashioned advertising was based on such simple selections, e.g., by sending marketing information on (say) hearing aids to all people in a particular area over the age of 70, or to readers of a magazine mostly read by older people.

Such coarse profiles may even be relied on subconsciously, reflecting even unknown (suppressed) prejudices. Thus, UK police in certain parts of London in the 1970s were reported to disproportionally "stop and search" young black men, clearly on the basis of preconceived notions that such individuals fitted a stereotype of a particular kind of criminal.

However, the "new" profiles used in the new global technical environment described in Working Paper No. 1 are (at least on their face) much more sophisticated. The novel feature is statistical analysis and weighing.

Essentially, modern profiles (like the old ones) consist of a list of factors linked to a particular issue or outcome, but with each factor given a certain, possibly dynamic weight. Thus, a profile of a typical buyer of lager beer might include such factors as age, place of residence, gender, height/weight ratio, social- and income group, etc., with some factors (say place of residence) being given more or less weight than others (such as, say, age). The weight attached to some factors may depend on other factors: the relative weight of certain factors for men may, for instance, differ from the weight accorded to the same factors for women. And the whole system may be dynamic, in that feedback loops can constantly correct the relative weights, to take account of new information. The overall calculation will almost invariably be carried out by computer, with the end result appearing to the user (that is, usually, to the organisation who wants to use the profile to "target" a particular kind of person) as little more than a complex algorithm.

The police and secret services increasingly "trawl" through databases and other data resources (or at least would like to trawl through them, if the law allowed it) in order to "match" all those in those databases against a pre-determined (but dynamically updated) "profile". We are all increasingly under surveillance, in the absence of any specific indication of guilt of any criminal offence.[97]

Here, it should be noted that the profiles used in this manner suffer from built-in biases of which even the software producers are often unaware,[98] or that may only become apparent if these programs are used in practice - and in the latter case only if their operation is adequately monitored for such distortions. But for that, it is necessary to truly understand the algorithms and programs. These, however, are effectively inaccessible (purportedly, for national security or even "commercial confidentiality" reasons). Even if they were to be made available, they would usually be incomprehensible and impenetrable to most.

The main point to be made here (before turning to more specific data protection related issues), is that these technologies are not infallible - on the contrary, they are subject to serious, inherent limitations and biases. "Profiling" and "data mining" may seem to work up to a point, but *inevitably* lead to actions against very large numbers of innocent people, on a scale that is both unacceptable in a democratic society and renders the "trawl" useless.[99] It is important to stress the inevitableness in this: this is not something that can be fixed by better design: attempts to identify very rare incidents or targets from a very large data set are mathematically certain to result in either an unacceptably high number of "false positives" (identifying large numbers of totally innocent people as suspects) or an unacceptably high number of "false negatives" (not identifying many real criminals or terrorists). This is referred to scientifically as the "base-rate fallacy"; colloquially (though less accurately), as: "*if you are looking for a needle in a haystack, it doesn't help to throw more hay on the stack*."[100]

Similar, if perhaps not quite so dangerous, misplaced reliance is increasingly placed on "profiles" in other areas: e.g., by public authorities, in order to identify children who are likely to grow up to become criminals (which in reality has the effect of stigmatising such children early on, which in turn becomes a self-fulfilling prophecy), or even in order to predict which of them may not reach "their full potential";[101] and by private bodies, to select or exclude people for or from offers of credit, mortages, or even employment. We believe that in the new global-technical environment described in Working Paper No. 1, the use of profiles will increase significantly, perhaps vastly, in both the public and private sectors; and that in both, there will be increased reliance on data from either sector, indeed from any source whatsoever.

"Profiling" thus raises serious societal questions. These are also reflected in data protection law; and data protection law and principles can help to address them.

The first main question is whether a "profile" constitutes personal data. On its face, one might think that it isn't: a "profile", after all, is essentially just a pulling together, in a single (possibly dynamic) algorithm, of a series of statistical findings (or perhaps it is better to say, assumptions and probabilities), perhaps derived from data on people, but not as such related to any one identifiable person.

However, that would be to ignore the purpose or effect of "profiles", in the senses discussed earlier, under the heading "identifiability". There is no doubt that, irrespective of whether the data used in the "profile" directly, in their "content", "relate" to individuals, they are (i) specifically intended to be applied to individuals, and (ii) can have extremely serious, indeed devastating effects on individuals found to "match" (or sufficiently match) a "profile": they can be denied a job or credit, placed on a "no-fly" list or even arrested on that basis. In other words, "profiles" meet at least two of the alternative criteria for determining whether data "relate" to a person, and must therefore be regarded as "personal", and thus whether data protection law applies: the criteria of "purpose" and "result" (or effect).[102]

This means that "profiles" - i.e., the data used in creating "profiles", and the processes through which they are created and used - should be fully subject to data protection law. In later sections, we will specifically draw attention to the implications of the various matters under discussion to the use of profiles. Specifically, we will return to them in the contexts of "fairness" in data processing, data quality (when is a profile "accurate"?), transparency (what should one be told about them?), general data subject rights (how can one challenge an impenetrable algorithm?) and the special (but rather underdeveloped) right not to be subject to fully automated decisions, etc. Here, it is enough to say that we believe this is one of the core issues to be addressed in the area of data protection in the new global-technical environment we are entering. We note that in the Council of Europe, efforts are under way to adopt a special Recommendation on the issue.[103]

(b) The Concept of "Personal Data" And "Data Subject", And The Issues of Anonymisation, Pseudonymisation, Re-Identifiability And "Profiling", In The National Laws:

general:

The national laws of the Member States all effectively repeat the definitions of "personal data" and "data subjects" as used in the Directive.[104] Moreover, the general approach of the Working Party, described in sub-section (a), above, reflects the approach taken by the national data protection authorities on the interpretation and application of these concepts.

There is thus quite widespread agreement in principle on the criteria to be applied in determining whether certain data are "personal data", i.e. whether they "relate" to an "identified" person; all will in principle accept the criteria of "content", "purpose" and "result" (or "effect") (even if the DPAs do not all spell them out). Such differences as there are tend to stem from either a strict, or a more "pragmatic" application of these criteria. Some countries, such as the UK and the Netherlands, are relatively lax in this regard, and will not actively seek to apply their law to processing operation which they feel do not merit it, while others, such as Germany and France (sometimes dismissed by the former as "too legalistic"), tend to first determine that the law applies, and only then are willing to examine ways in which the terms of the law can be applied flexibly (which is often of course possible). However, the differences should not be exaggerrated. For instance, the question of "result", i.e. of whether (processing of) certain data can have an effect on individuals allows for discretion under either approach.

The issue of data on "things" more or less closely linked to individuals (noted at (a), above) has also been addressed at the national level, in respect, e.g., of IP addresses, digital pictures of properties, and telephone numbers. Thus, in the Netherlands, it has been 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. In France, in the past, Internet access providers were deemed to hold personal data if they linked IP-addresses to users, but not if such links were not retained. We will return to this a little later.

Also in the Netherlands, the data protection authority held some years ago that pictures of properties in a major database covering all Dutch streets through 360º digital camera recording constituted personal data if they were used in such a way as to have repercussions for individuals (such as owners or occupiers), e.g. if they were to be used for valuation or taxation purposes, but not if they were not so used. However, in the light of the controversy, in many European countries, over Google's "*Streetview*", this view may well be revised, if only because (at least on "*Streetview*") such data are now not just held in a database, with some control over access and use, but uploaded to the Internet, where anyone can access the data and link them to any other data they have access to.

In Sweden, under both the current and the previous law, telephone numbers are normally regarded as "personal data". 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. However, it is doubtful whether that view would still pertain, especially if the file were to be released in digital format, more especially if it became accessible on-line.

The new technological developments thus everywhere naturally continue to shape the application of the law; the law in this respect is everywhere in flux. "*Πάντα ῥεῖ*", as Heraclitos is supposed to have said (but probably didn't).[105]

This could also affect the question of retention of IP addresses in "un-linked" format, i.e., which are not linked to a person by the main controller (in the above examples, the creator of a CD-ROM and more typically an ISP). In the new global-technical environment described in Working Paper No. 1, consideration should be given to the possibility of other data later being linked to the "unidentified" IP addresses, and to data linked to the "unidentified" addresses. For instance, if the ISP retained a long-term record of all websites linked to the IP addresses, that would make the supposedly, for the time being, "unidentified" data (IP addresses and visited websites) potentially highly sensitive: if the IP address could later be re-identified with the user (or at least with the PC of the user), it would create a very intrusive personal record. The means for breaking anonymity, briefly described by Professor Anderson above, make this a very real possibility in the new global technical environment. The view of the DPAs that retention of IP addresses does not raise data protection issues as long as they are not (at the time of assessment) linked to individuals (or PCs of individuals), thus becomes too complacent. The only way to ensure proper data protection is to delete IP addresses as soon as possible, rather than to keep them in (supposedly) anonymised form.[106]

Further core issues for the present study are the questions of anonymisation, pseudonymisation and re-identifiability, and "profiling", discusses in the last sub-headings under (a), above.

"*anonymisation, pseudonymisation and re-identifiability*":

Several countries include specific definitions of, or relating to, the above-mentioned concepts in their laws. Thus, 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, under their law, *may* in certain circumstances not be linked 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 - especially in the laws which use such flexible language - 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." These terms appear to be absolute, with encoded data no longer to be given any special, relaxed treatment under the law if there is *any* possibility of them being re-identified. As we hope we made clear in sub-section (a), above, such absolute impossibility of re-identification is in reality almost impossible to achieve (and will be even less possible in the new environment). In practice, the authorities in these countries are likely to make some allowances in this regard, but with a tendency to be strict.

The approaches in the different countries also rest to a large extent on the question of whether the national law, or the national DPA, considers the question of "identifiability" as relative, in the sense that encoded or pseudonymised data are regarded as identifiable in relation to a person with the "key", but not in relation to anyone who does not have the "key" (or other means to re-identify the data).

The latter approach appears to be taken by most countries, including Austria, Germany, Greece, Ireland, Luxembourg, the Netherlands, Portugal and the UK.

However, 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.

This is clearly an area in which further guidance and approximation is necessary, in particular in view of the increasingly international transborder dissemination of pseudonymised or (supposedly) anonymised data, for scientific research, marketing research and other purposes.

The question of "applicable law" here again becomes crucial, and contentious, if the rules in countries with a relatively "strict" approach could be circumvented by controlling processing operations from countries with more relaxed views. For instance, if data could be collected in encoded form directly from a "strict" EU Member State by a controller in a "less strict" Member State, or transferred from the "strict" Member State to that other EU Member State on the basis of the principle of free data transfers within the EU, only to be then further transferred to a third country, in contexts in which the data could not have been disclosed (even in encoded form) within the first country, or sent from the first to the third county.

"*profiling*":

The question of "profiling" has, in mosty countries, only recently come to the forefront of the domestic discussions; most references on DPA websites are still limited to a general discussion of the problems the phenomenon raises and the threats it poses. However, the issue has a long history in Germany, where (rather basic) forms of "profiling", or "*Rasterfahndung*", were tried out in the 1970s against the terrorist group the "Red Army Faction" (RAF). The Constitutional Court has recently had to deal with the revival of these methods.

The case concerned the search, by the German police, for possible further "sleepers" from Islamist terrorist cells, after it had been discovered that one group of perpetrators of the "9/11" attack on the World Trade Center in New York had been living in Germany under the guise of studying there. The police asked the local authorities keeping records of foreign residents for details of all foreign students from 23 Islamic countries of origin, and to obtain further details from the universities where they were enrolled. A Moroccan student challenged the data search, and the case was ultimately dealt with in the Constitutional Court.[107]

The Court held that the lower courts' decisions that held that the police actions were lawful, had violated the constitutional (data protection) rights of the student. The Court's reasoning can be summarised as follows:[108]

> A preventive police search based on a "profile" [*eine präventive polizeiliche Rasterfahndung*] is only compatible with the fundamental right to informational self-determination when there is at least a concrete danger [*eine konkrete Gefahr*] to high-ranking legally protected matters [*Rechtsgüter*], such as the integrity or the security of the [German] Federation or one of its States, or to the life, limb or freedom of an individual. It is not in accordance with constitutional requirements [such as the principle of proportionality - DK] to carry out such a "profile"-based search as a mere general-preventative measure [*bloße Vorfeldmaßnahme*]. Neither a general threat, such as has been present continuously since the 11th of September 2001 in view of the terrorist

> attacks [on the USA, on that date], nor international political pressures, suffice [to allow such a search]. Rather, further facts must be present, that indicate a concrete danger, for instance that terrorist attacks are [actually] being prepared or predictably to be carried out.

The Bavarian data protection authority drew the following conclusions from the judgment, relevant to the present study:[109]

- "Profile"-based police searches of databases should only be permissible if there is at least a concrete danger to high-ranking legally protected matters, i.e., if there is real, factual evidence of such a direct threat;

- Independent from the approval of such a measure by the Executive (in the Bavarian case, the Ministry of Interior Affairs of that State), the measure should require the authorisation of a judge;

- The uses to which the thus-obtained data can be put must be specifically and precisely determined, and any use of the data for other purposes must be noted and recorded;

- In view of the covert nature of the "profile"-based search, the rule should be that those that have been put under surveillance in this way, or at least those whose data are retained in the overall dataset at the end of the search, should be informed: "the guarantee of effective protection of the relevant constitutional rights demands such informing, so that the data subject has access to legal challenges [to the measure, and to any data retention or use.]"

The DPA adds, significantly, that: [110]

> The considerations of the Constitutional Court can also be relevant for other police measures which - like "profile"-based searches - are marked by both being applied in the absence of specific suspicion [against each individual caught up in the "trawl" - DK] and by their broad application, i.e. for measures through which numerous people are caught, [but] which is not in any way related to any wrongdoing on their part, and who have in no way caused the [application of the] measure to them, such as automatic car licence plate recognition systems.

The above is quoted here at some length, because it shows the important constitutional-legal implications of the use of "profiles" and other "broad-spectrum" "trawling" through personal data, at least in some countries. Although the specific issue addressed in Germany was police investigations, which of course require special restrictions and safeguards, we believe that there are also lessons here for the use of "profiles" in other contexts, notably by other public authorities (such as the identification of children "likely" to fail at school, or become pregnant, or grow up to become a criminal). Indeed, we believe that not very different considerations should apply to the use of "profiles" in other contexts in which individuals can be seriously affected by them, such as in employment, housing or credit. It must also again be noted that, increasingly, there is matching of databases in different sectors, private and public, "profiling" using both.[111]

Here, we may limit ourselves to noting that, again, these matters touch on important constitutional matters in some countries (apart from Germany, at least also in France, Spain, Italy and others). The issues can only be resolved at the EU level if the outcomes meet at least the standards of the constitutional requirements in those countries.

All of this is also becoming more urgent and pressing now that the Lisbon Treaty has abolished the previous three "pillars".

"PROCESSING [OF PERSONAL DATA]":

(a) The Concept of "Processing" In The Directive:

The original draft of the Framework Directive had as its core concept the notion of "[personal data] file" or "filing system," in line with the core concepts of *fichier* and *Datei* in the original French and German data protection laws of the 1970s. The Directive retains this concept but defines it broadly to cover all filing systems that are in any way "structured." However, since this concept was no longer considered to be adequate to deal with more modern, dispersed and transient computer operations, the core concept was changed to "processing" in the final version of the Directive. This concept is defined in Article 2(b) of the Directive as follows:

> "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

The term processing here is clearly defined very widely to include not just "technical" processing but also the collection, recording, consultation, and destruction of personal data. Importantly, it also includes the processes of pseudonymisation and anonymisation of data: as a result, controllers are not just free to pseudonymise or (supposedly) anonymise any data they hold, and then escape the law; rather, in doing so, they must comply with the relevant legal requirements for lawful processing. They may thus, for instance, need to inform the data subject, or indeed obtain their consent for this processing.

This change of core concept in data protection from "file" to "processing" also means that the crucial substantive and formal requirements of the directives apply not to the owner (or user or holder) of certain personal data or of a particular computer file or filing system (as under most previous laws), but to the "controller" of a particular processing operation, that is, to the natural person or legal entity (company) that "determines the purposes [and means]" of the processing operation in question, as discussed in the previous sub-section.

Moreover, as discussed in Part 3 of this paper, above, the crucial question for the determination of the "law applicable" to any particular processing operation is not the law of the physical location of the relevant filing system or computer, nor indeed necessarily the law of the country in which the processing takes place, but (in the convoluted wording of the Directive) "the place of establishment" of "the establishment of the controller," "in the context of the activities of which" the processing takes place.

While this is in itself reasonably clear, we feel there is still a considerable amount of clarification to be done in this respect *vis-à-vis* organisations involved in the processing of personal data, especially if they are part of a complex international company or group of companies, or operation. In particular, it should be made clear to them that (as discussed in sPart 3, above) even within the EU, different national laws may apply to different processing operations they are involved in. Processing carried out purely within the context of their own activities will be subject to their local laws only, but if they are involved in processing on behalf of other entities within their international corporation or group, those other operations may be subject to different laws (only, or as well).

(b) The Concept of "Processing" In The National Laws:

The laws in the Member States studied all contain definitions of "processing", but with a significant amount of minor and not-so-minor variations, omissions or additions. Thus, the laws in Belgium, France, 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").[112]

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, 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 law in Ireland 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*. 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" in Article 2(e)). 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.

"CONTROLLER" AND "PROCESSOR":

(a) The Concepts of "Controller" and "Processor" In The Directive; the link with Binding Corporate Rules:

The concepts of "controller" and "processor", and the distinctions between the two, are important, in that their respective duties and responsabilities differ. The former is furthermore crucial to the proper application of the Directive in a transnational context, in that, as we have seen in Part 3, the place of establishment of the controller is largely determinative of the "applicable law".

"*controller*":

The definition of "controller" in Article 2(d) of the main Directive reads as follows:

> "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

We will leave aside the question of controllers specified by law; that is something usually used to overcome the problems of legal demarcations in State institutions, to clarify which department or governmental- or quasi-governmental body (such as a national health service) shall be responsible in data protection law for certain processing operations.

As far as the main definition is concerned, it is usually, in current ordinary contexts, not difficult to identify the controller of a particular processing operation. However, there are a number of ambiguities in the definition which can cause problems, and these problems are likely to increase in the new global technical environment described in Working Paper No. 1.

First of all, the definition appears to assume that there is always only one, defined entity that "determines" both the "purposes" and the "means" of any processing (processing operation). In practice, an organisation that wants to carry out a particular processing operation will indeed usually "determine the purposes" of that operation. However, it may well leave the choice of "means" to achieve those purposes to others, such as any agents it may engage. A sensible way to resolve this would be to hold that the primary criterion for determining who (which person or entity) is the controller, is to see who determined the purposes of the

processing; and to read the reference to "means" as indicating that the controller will also be responsible for the means that are chosen to achieve those purposes (even if in practice this choice can be delegated to others).

Another ambiguity stems from the fact that the Directive, in the definition, stipulates that the controller can make these determinations "alone or jointly with others". As noted earlier, this could be read as suggesting that for some operations, there can be "joint controllers". As we shall see in sub-section (b), below, this is a reading that is supported by some national laws (but not by others). However, such a reading seriously complicates the "applicable law" determination, if there were "joint controllers" based in different countries: as we have seen in Part 3 of this paper, above, the Directive, in the main rules on "applicable law" in Article 4, assumes that there is just one controller for each processing operation.

We feel we may therefore here repeat our suggestion that perhaps a better reading would be that in spite of the reference to a controller acting "alone or jointly with others", there still always is only one controller for any specific processing operation, who may however involve others in making the determinations about means and purposes (perhaps especially the means). If several entities were involved, "the" controller would be the one entity that had, or if that is not clear, formally took, responsibility for determining the purposes of the processing.

However, we accept that others might take a different view. We believe the Article 29 Working Party could provide useful guidance on these matters, but in our Final Report will also further reflect on this.

"*processor*":

The concept of "controller" is furthermore closely related to the concept of "processor". The latter is defined in Article 2(d) of the Directive, as follows:

> "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

In other words, a processor is essentially an agent of the controller. This is confirmed in paras. (2) to (4) of Article 17, which stipulate the following:

> (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:
>
> 1. the processor shall act only on instructions from the controller,
> 2. the [data security and confidentiality] 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.

In practice, it is sometimes difficult to discern exactly who is a controller and who a processor. This occurs in particular in complex international organisations such as multinational companies or groups of companies, which are often made up of a large number of variously-related entities, with complex links and arrangements between them. Such entities are often not clearly hierarchically structured: some (perhaps many, perhaps all) associated entities may be subject to some centrally-determined policies, e.g. on postings, pensions and careers, but largely autonomous in other respects, e.g. in relation to marketing or customer care. In terms of data processing in particular, there may be numerous complex technical arrangements: entities belonging to the multinational in one country, say in Europe, may well send "their" data to another entity (perhaps the global headquarters, perhaps not) in another part of the world, and *visa versa* - quite simply to make best use of computer capacity during night hours in these different parts of the globe. Sometimes, there are impermeable firewalls between the data thus processed on behalf of the different entities - and in that case, the roles of controller and processor can perhaps still be relatively clearly determined. But sometimes, data that are being sent for processing to another part of the world may also be retained or copied by the entity doing the processing. This is not always entirely clear (sometimes not even to the data exporting entity). It can be extremely difficult to map the complex dataflows within such organisations, break them down in relation to distinct processing operations (defined by the different purposes of those operations: see above), and then determine who is the controller of which operation, and who a processor - and thus, *inter alia* (but not least) what law applies. What is more, it follows from Article 17(4) that many of these relationships will have to be written up in binding legal contracts (or - equally binding and written - intra-corporate agreements). The drafting of such documents is far from simple - and they may need to be kept under constant review, in the light of changing group- or corporate policies.

"*Binding Corporate Rules*":

This issue is supposed to be addressed through the new mechanism, still under discussion, of "Binding Corporate Rules" that can be assessed and approved at the EU level. We believe that that is indeed an important attempt to resolve the issue. However, given the complexities, and the always quickly-changing corporate environment (as a result of restructuring, mergers and acquisitions, and indeed business failures), both the drafting and the assessment, and keeping up to date, of such rules is likely to be extremely time- and money-consuming (the approval of European codes of conduct has proven to be a limited tool precisely because of these demands, and they need less constant revision). In the increasingly globalised economy, the need for such rules, and such assessments, will furthermore increase starkly (even in the current economic downturn). It remains to be seen whether BCRs will therefore really provide an answer to these complex questions for all but a small number of major corporations.

In our Final Report, we will further examine how and to what extent BCRs can be used in this way, and (perhaps more importantly) if there are other, more efficient - and cheaper - options.

(a) The Concepts of "Controller" and "Processor" In The National Laws:

"*controller*":

Even if we again leave aside the question of a controller being determined by (national) law,[113] there are still some notable differences between the national laws in the definitions of "controller" and "processor".

Some laws follow the definition of "controller" in the Directive closely: this is the case in, e.g., Belgium, Denmark, Luxembourg, the Netherlands and Sweden. However, the definitions in the laws of other countries divert somewhat from the text of the 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.

The law in Spain refers to the controller as the person who determines the "purposes, *contents and use*" of the processing. The law in Ireland defines the controller as the person who "either alone or with others, *controls the contents and use* of personal data". The Greek law defines the controller as the person who determines the "*scope and manner*" of the processing. 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 ..." The post-Directive law in Germany changed the term used in the previous law 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 buildt 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").

By contrast, the Austrian law defines the controller, in line with our suggested interpretation of the definition in the Directive, quite simply 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 (the law 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, but that is a different issue).

In practice, these divergencies do not appear to have caused any great differences in the determination of the controller, but they are still unhelpful to the aim of harmonised (or at least approximated) application of the Directive. In any future regulation or guidance, closer approximation would be useful.

"*processor*":

The concept of "processor" is defined in exactly the same terms as are used in the Directive in the Luxembourg and Portugese laws, and in effectively the same terms in the laws in Belgium, Denmark, Greece, Italy, the Netherlands, Spain, Sweden and the UK. 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).

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 or agent, rather than the original controller (i.e. the person who instructed the processor, the principal) 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" to "someone who processes personal data on behalf of [the controller]". The French law refers to a "processing agent" (*soustraitant*) in its (somewhat odd) definition of "recipient" and stipulates in the rules on processing by such agents that the term covers "anyone who processes personal data on behalf of the controller".

The German law deals separately, and 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.

Overall, the application of the national concepts throws up the same problems about who is to be regarded as the controller, and who as a processor, as were discussed above, at (a), with reference to the definitions in the Directive.

For the future of data protection in the EU (and beyond), it will be important to clarify and harmonise these concepts, in the manner suggested at (a), especially if the central factor for the determination of the law that is applicable to any particular processing operation remains the place of establishment of the controller, in the context of the activities of whom the processing takes place.

4.2 THE DATA PROTECTION PRINCIPLES

(a) The Data Protection Principles In The Directive

What the Directive call the "principles relating to data quality" are in fact general principles not limited to the "quality" of the data only. They derive directly from the principles contained in the Council of Europe Convention on data protection (Convention No. 108), but they also expand somewhat on those principles. Briefly, they state that personal data must be:

- processed fairly and lawfully (Art. 6(1)(a) of the Directive; cf. Art. 5(a) of Convention No. 108);
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Art. 6(1)(b) of the Directive; cf. Art. 5(b) of Convention No. 108);
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Art. 6(1)(c) of the Directive; cf. Art. 5(c) of Convention No. 108);
- accurate and, where necessary, kept up to date (Art. 6(1)(d) of the Directive; cf. Art. 5(d) of Convention No. 108); and
- kept in identifiable form for no longer than necessary for the purposes for which the data were collected or for which they are further processed (Art. 6(1)(e) of the Directive; cf. Art. 5(e) of Convention No. 108).

These principles centre on two core concepts. The first is "purpose specification and limitation"; the second is "fairness."

Purpose specification and limitation

It is one of the central features of the Directive (and of data protection in general) that it restricts the processing of personal data by reference to the purpose or purposes for which the data are collected. Indeed, a processing operation is basically defined by reference to its purpose(s). What is more, as is made clear in Article 6(1)(b) of the Directive, these purposes should be clarified "explicitly" in "specific" terms. It is thus clearly incompatible with this principle to build up a large database on an entire population for general, not prespecified, uses, i.e., a data resource to be "mined" for whatever valuable information may be extracted, for whatever purpose.

According to Article 6(1)(b), the "specified" and "explicit" purpose must also be "legitimate." This is not the same as lawful: Certain activities may be technically within the law but nevertheless not "legitimate," e.g., if they have unfair or disproportionately negative effects on the data subjects. This ties in with the requirement of "fairness", noted below.

The most important consequence of the specification of a data processing operation's purpose (or purposes) is that it determines the uses to which the data in question may be put. They may, first of all, be used for the "legitimate," "specified" purpose or purposes in question, provided that the other requirements of the relevant directives, such as the informing of data subjects, or the exercise of data subjects' rights, or transborder data flow regulations, have been complied with. However, Article 6(1)(b) also allows for the use of personal data for

other than the original, specified, primary purpose, to the extent that the further processing is "not incompatible" with the primary purpose.[114]

The Directive also limits the nature and amount of data that can be collected by stipulating that the data must be "relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Art. 6(1)(c)). The adequacy, accuracy, up-to-dateness, relevance or excessiveness of personal data is also to be assessed by reference to the specified purpose or purposes. As the Directive puts it in Art. 6(1)(d), "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.[emphasis added]" Data that are "adequate" or sufficiently accurate or "complete" for one purpose may therefore well be inadequate and insufficiently accurate or complete for other purposes. And finally, data may only be held for so long as is necessary for the purpose(s) for which they were collected or further used. The data retention period is, therefore, also linked to the specified purpose: data held for one purpose may be kept for longer, or less long, than data kept for other purposes.

Fairness

The very first requirement, stipulated in the first data protection principle set out in Article 6(1)(a) of the Framework Directive, is that personal data must always be processed "fairly and lawfully." The requirement of lawfulness is relatively straightforward: of course, all processing of personal data, like any other activity, must conform to the law, although it should be stressed that this refers not only to data protection law but also to other legal requirements such as may flow from contract law, consumer law, or employment law (to name but a few).

However, the Directive goes further by adding that all processing of personal data must also be "fair." By common law standards this is rather vague, although, of course, the concept of "unfair competition" is known. In Continental legal thinking, the general application of such a broad standard is much more common, by reference to a variety of terms such as *loyal* (F), *leal* (Sp), *nach Treu und Glauben* (D), *eerlijk* (NL), as opposed to the narrower *licitement*, *licita*, *rechtmässig*, *rechtmatig*, etc. In this way, the test of "fairness" builds on the equally broad requirement, discussed earlier, that all processing must serve a "legitimate" (rather than just a "lawful") purpose.

The requirement of "fairness," therefore, creates a sort of legal "safety net" underneath all the other, more specific requirements of the Directive. Processing can, in theory, meet all the specific requirements of the Directive (or of any of the national laws implementing the Directive) yet still be "unfair" and, therefore, not allowed.

Clearly, all of the above tests ("compatability", "legitimacy", "relevance", "reasonableness", "fairness") allow for wide margins of appreciation: their application in practice is likely to vary, as indeed we shall see in the next sub-section.

(b) The Data Protection Principles In The National Laws

The data protection principles are contained in the laws of all the Member States studied, 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 (discussed below, at 4.3) 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 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 studied. 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 particular for public-sector controllers. In others, purposes are sometimes defined in excessively broad terms, thus undermining the principle itself. For instance, UK law refers to "policing purposes" in one breath (and thus allows data obtained for one police purpose to be used for any such purpose), where German law strictly distinguishes between "countering immediate threats", "general and specific prevention", and "investigation and prosecution of [suspected] criminal offences".[115] More blatantly in violation of the Directive, the UK Data Protection Act adds "medical research" to the list of medical purposes set out in Article 8(3) of the Directive, thus circumventing purpose-limitation in that regard (contrary to the clear guidance on this from the WP29).[116]

The rules concerning secondary processing of non-sensitive personal data for research purposes without the consent of the data subjects also vary very considerably. Some Member States 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, which 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" (see at 4.4, below).

4.3 THE CRITERIA FOR LAWFUL PROCESSING

(a) The Criteria For Lawful Processing In The Directive

Article 7 of the Directive sets out a list of "criteria for making data processing legitimate" (referred to in earlier drafts of the directive as "grounds for lawful processing"). For any data processing to be lawful, it must be based on one of these "criteria" or grounds. It is important to stress that Articles 6 and 7 apply cumulatively: Processing of (non-sensitive) personal data must both conform to the data protection principles set out above, at 4.2, **and** it must meet one of the following "criteria":[117]

- the data subject has "unambiguously" given his consent (Art. 7(a) of the Directive);
- the processing is necessary in a contractual or precontractual context (Art. 7(b));
- the processing is necessary for compliance with a legal obligation (Art. 7(c));
- the processing is necessary to protect the vital interests of the data subject (Art. 7(d));
- the processing is necessary for the performance of a task in the public interest or in the exercise of public authority (Art. 7(e)); or
- the 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, unless these interests are overridden by the interests or fundamental rights and freedoms of the data subject (Art. 7(f), the so-called "balance" provision).

In other words, processing of personal data is only allowed if, either, it is carried out with the consent of the data subject, or it is "necessary" in a contractual context or for some overriding (in particular public) interest, or if a "balancing" of the interests of the data user (or possibly a third party) and of the data subject has shown that the interests of the first should prevail.

Processing of personal data in relation to commercial activities will usually be based on consent, contract or "balance", while processing in the public sector will mostly relate to the performance of a "public task" or the exercise of "public authority", but the boundaries are not sharp. Both public- and private-sector controllers can be obliged to process personal data under a "legal obligation", or may do so to protect "vital interests" of the data subject.

In this brief overview, it must suffice to note that this provision reflects the structure of the main substantive articles in the European Convention on Human Rights (ECHR), which allow for restrictions on, or "interferences with", such rights for a "legitimate purpose" (of the kind mentioned or clearly referred to in paras. (b) – (f)), provided that the restrictions or interferences are "necessary in a democratic society". The European Court of Human Rights has developed detailed tests on the basis of this approach, which therefore also apply under the Directive, in the application of these criteria.[118] We will return to these below.

(b) The Criteria For Lawful Processing In The National Laws

The "criteria for lawful processing" are contained in the laws of all the Member States studied, 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,

Ireland, Luxembourg, the Netherlands, Sweden and the UK - but in Finland they are set out in the middle of the data protection principles (discussed above, at 4.2), while in the UK law they are linked to the "fair and lawful processing" requirement (which means that if one of the criteria is met, the question of fairness and lawfulness is effectively left aside).

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 criteria are seen as exceptions to these primary criteria. In the Czech Republic, France, 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 is the case 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. Here, we will limit ourselves to very brief discussions of processing on the basis of statutory authorisation, processing on the basis of consent, and processing on the basis of the "balance" criterion.

processing on the basis of statutory authorisation[119]

Many national laws repeat the criteria relating to legal obligations, tasks and powers in terms identical to, or very similar to the ones used in the Directive. In terms of the ECHR, they relate to processing of personal data (which, in terms of the Convention, *ipso facto* constitutes an "interference" with private life) that is provided for by "law". This means that the legal rules on which the processing is based must meet the detailed requirements of "law" and "necessity" that the European Court of Human Rights has elaborated in extensive case-law. Simply put, the Court has set certain "quality" standards for such law: the relevant rules must be accessible, clear, precise and foreseeable in their application, and prevent arbitrariness; they must serve a "pressing social need"; they must be proportionate to that need; and they must provide for effective redress (especially if they leave a certain discretion in the hands of the relevant controllers).[120] In the last few years, the European Court of Human Rights has, on several occasions, ruled that national laws allowing for the processing of personal data did

not meet these quality requirements. These cases also raised doubt about whether the purpose(s) for which the personal data were being processed was (were) defined in sufficiently precise terms.[121]

If serious problems are to be avoided, it is essential that further clear guidance be given on the quality of laws authorising the processing of personal data, and on the requirements of necessity, specificity and proportionality in this respect. It is clear that in several Member States, legal rules that are relied on to allow processing (and sharing, and "data mining") of personal data, especially in the public and quasi-public sectors, do not meet these standards.

This will cause problems in purely domestic terms, but also (and of more importance to this study) in relation to other States, and the EU, if such deficient laws were to apply extra-territorially as a result of the "applicable law" rules, discussed in Part 3, above. This is certain to become much more common in the new internationalised environment, in which data processing will increasingly become subject to national laws of other countries than the place where the data subject is resident (or where he or she happens to be when the data were obtained). One can think of collection of personal data on-line or by SMS or over the telephone for ill-defined purposes, but also of disclosures of personal data by a public authority in one country to an authority in another country, e.g., in relation to medical treatment or (much more problematic) research, or social welfare benefits, or welfare fraud detection, or asylum or police matters, of the sale of such data by a private body in one country to another in another country, as well of course as of transnational public-private sector data exchanges (as in the case of PNR data). If the disclosure or sale is based on a "law" in the originating country that does not meet the ECHR requirements - and thus, we submit, *ipso facto* also not the criteria of Article 7(b) or (e) - the processing may not be regarded as lawful by the country in which the recipient is established (even if the "law" of the country of the body disclosing the data [wrongly] allowed the disclosure and transfer).

processing on the basis of consent

In terms of "informational self-determination", processing on the basis of consent is clearly crucially important, but with the *caveat* that (as it is put in Article 7(a) of the Directive) such consent must be "free, specific and informed". Yet again, in spite of this being such a core issue, the matter is not dealt with uniformly in the Member States. Thus, 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); the Luxembourg law even 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").

The French, Irish and UK laws all fail to define the concept of "consent" - but they do of course refer to it in their list of criteria. However, they differ in their application of the criterion. In France, 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 - 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.

By contrast, in the UK law, the provision allowing for processing of (non-sensitive) personal data merely mentions (undefined) "consent" as one condition for processing - which contrasts with the condition for processing of sensitive data which refers to "explicit consent". 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. Similarly, the Irish law says processing has to be based on *explicit* consent - but the data protection authority is more relaxed in relation to processing for a clearly-understood - and well-defined - purpose, than about processing for non-obvious secondary purposes, and allows implied consent in the first context.

In Germany, a request for consent for a separate purpose than the primary purpose must be especially 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: in Germany, this is regarded more as a matter to be resolved interms of "unfair" (invalid) terms and conditions than as a data protection issue, but stricter rules under the data protection law are due to come into effect in 2010.[122] 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 is 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.

Special issues also arise in relation to consent by minors. This has been dealt with in some detail in some special contexts, in a few countries (e.g., Denmark), but remains a matter that is not yet fully clarified, either in national law and practice, or in guidance from the WP29 (although the latter has issued a preliminary paper on the topic).[123]

All these divergencies will yet again become more problematic in the new, generally-internationalised environment, including the Internet. "Consent" obtained under the law of one country - the "applicable law" at the time of data collection - and valid under that law, may well be regarded as insufficient and invalid if relied on for subsequent processing in another country (even another EU/EEA Member State), e.g., because (in the view of the second country) the original consent was insufficiently specific, or obtained under what the second country regards as duress, etc. The situation is of course even more problematic if the first country is a non-EU/EEA State.

There is some limited European guidance in respect of consent, in specific context, such as transborder data flows,[124]employment,[125]schools,[126] and medical care. To take the latter as an example, the WP29 has expressed the view that:[127]

> Consent must be specific: 'Specific' consent must relate to a well-defined,concrete situation in which the processing of medical data is envisaged. Therefore a'general agreement' of the data subject e.g. to the collection of his medical data for anEHR [Electronic Health Record] and to subsequent transfers of these medical data of the past and of the future tohealth professionals involved in treatment would not constitute consent in the terms ofArticle 2(h) of the Directive.

Clearly, this has, to date, not yet resolved the issues.

processing on the basis of the "balance" criterion

The "balance" criterion (Article 7(f) of the Directive) is, by its nature, the vaguest and most open-ended of the criteria, and thus the one perhaps most in need of clarification as to how it can and should be applied in specific contexts. This is recognised in the laws of several countries (Belgium, Ireland, UK), which envisage the issuing of further rules on the application of the "balance" criterion in specific contects. However, remarkably, none of these have not actually issued such more precise rules.

Overall, there are also notable differences in approach to this criterion in the Member States. In the UK, it is largely left to controllers to determine for themselves whether they can process non-sensitive data on this basis. This is in theory subject to supervision by the data protection authority, but there are no published reports of the UK authority ever having taken any enforcement action over this. The criterion is consequently extensively relied on by controllers. In the Netherlands, the Explanatory Memorandum to the law adopted to implement the Directive set out the matters that should be taken into account in assessing whether processing can be allowed on this basis; it mentions: 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). Similar matters are taken into account in other countries.

In Germany, a "balance" test expressed in the kind of general terms used in the Directive applies only to the private sector. Somewhat similar, but more precisely-worded tests apply in the public sector, but these in fact get closer to the application of a "necessity" test.

Other countries generally apply more-strictly-phrased test, or impose strict procedural requirements on processing on the basis of this criterion. 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 mainly (almost only) 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 credit-worthiness, and on data used for insurance purposes, which also lay down guarantees aimed at striking a 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).

These divergencies can again cause problems in the new, generally-internationalised environment, if data are obtained on the basis of this criterion in one Member State, and then

transferred to another, in which the criterion is more restrictively applied - or indeed, if a controller in one country, which is relatively lax in its application of the criterion, tries to obtain data directly from data subjects (e.g., over the Internet, or by 'phone) on this basis, under the controller's national law, when the data subjects are in fact in another Member State with a stricter law in this respect. The relatively lax law of the country of the controller may well be the "applicable law" - but the country of the data subject may not be happy to allow data collection from (and on) its citizens, on its territory, on the basis of a vague rule which is much more strictly applied to controllers in that country itself, when they try to obtain data in the same way.

4.4 PROCESSING OF SENSITIVE DATA

(a) Processing Of Sensitive Data In The Directive

In Article 8, the Directive lays down certain additional (stricter) rules, over and above the general rules and criteria specified in Articles 6 and 7, concerning the processing of certain special categories of data, commonly referred to as "sensitive data". These distinguish between a group of main categories of such data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and data on health or sexual matters) (Art. 8(1)); data relating to criminal convictions and related or similar matters (Art. 8(5)); and the use of a national identification number or similar general identifiers (Art. 8(7)).

The Directive requires the Member States to impose an in-principle prohibition on the processing of the main categories of sensitive data (Art. 8(1)), subject to a series of exception clauses (set out in Art. 8(2)), which in effect amount to special conditions for the lawful processing of such data, similar to, but stricter, than the main criteria for lawful processing of non-sensitive data, discussed above, at 4.3 (but with the notable absence of a "balance" criterion or condition). Like the ordinary criteria for lawful processing, these special conditions are to applied cumulatively with the data protection principles, discussed at 4.2, above. The Directive adds some special exceptions allowing for the use of sensitive data by non-profit-seeking bodies with a political, philosophical, religious or trade-union aim (subject to certain conditions and to "appropriate guarantees", to be specified by the Member State), and for the use of such data for medical purposes (but which do not include medical research), and a further, open-ended provision allowing Member States to adopt yet further exceptions "for reasons of substantial public interest", "subject to the provision of suitable safeguards" (which must be reported to the Commission and the other Member States) (Art. 8(4) and (6)).

The provisions themselves raise many questions, including the question of what data are actually caught by the main categories. In that respect, the Article 29 Working Party has issued some guidance on, e.g., biometric data (which it also usefully defined)[128] and on the Human Genome and genetic data.[129] Otherwise, however, it must suffice to note here that, once again - but perhaps in this context even more than in others - the Directive expressly gives Member States considerable freedom to apply, restrict or extend the rules on sensitive data, largely as they feel fit, subject only to rather vague requirements that more relaxed rules in specific contexts are subject to "appropriate guarantees" or "suitable safeguards". However, on these, regrettably, there is no guidance.

(b) Processing Of Sensitive Data In The National Laws

Some Member States extend the special rules on the processing of sensitive data, set out in the Directive, to certain data not included in the list in the Directive. This concerns data on debts, financial standing and the payment of welfare (social security) benefits in particular. Some States also include data on criminal convictions etc. in the general list 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 (and in particular also on the basis of consent, which is not mentioned in Article 8(5) of the Directive). Apart from this, it may suffice to note the rules on the processing of sensitive data in some special contexts:

Employment: Although the laws in several of the Member States contain general 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 in most this has not yet been done. An exception is Italy, which in 2008 adopted an "Authorisation" Concerning Processing of Sensitive Data in the Employment Context.[130] Elsewhere, however, the situation in this regard is generally still very much determined by separate – and widely 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. This is also confirmed by a recent Comparative Study, commissioned by the EU Fundamental Rights Agency, which found that:

> The protection of personal data in the field of employment also needs to be enhanced, since only some Member States provide *ad hoc* regulation for this complex area.[131]

The WP29 has issued one general opinion on the processing of personal data in the employment context; a recommendation on employment evaluation data; and a working document on surveullance of electronic communications in the workplace; also relevant is its opinion on email screening services.[132] However, to date, these have not led to any major convergence (let alone harmonisation) in this respect.

Substantial public interest: Several of the data protection laws of the Member States studied 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 a very few Member States (in particular, the UK and France), and in the rules in question, at least in the UK, the standards are somewhat ambiguous.

Several laws similarly allow for the issuing by the national Data Protection Authority of specific *ad hoc* authorisations - but as far as we know the Commission has not been notified of any (as it should have been under Article 8(6) of the Directive). 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; to the best of our knowledge, no such permits have been applied for, at least by the major international human rights organisations.

It should be noted in this context, however, that 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. It is a moot question whether these other laws contain the "suitable safeguards" that should be provided in this respect, according to Article 8(4) of the Directive. Also, again, such other laws or provisions should have been notified to the Commission, but this does not appear to have been done to any great degree. This area therefore remains rather obscure, but it is clear that in many countries, in many respects, there must be serious doubts as to whether the rules comply with the Directive in this regard. What is more, it is also clear that given that these matters are regulated in so many disparate laws (mostly not drafted to deal with data protection at all), major differences remain between the laws in the different Member States.

Once again, this would have serious implications if such laws were to be relied on in circumstances in which the relevant national law was the "applicable law" in a transnational context. Until recently, this was perhaps not so urgent, since many matters of "substantial public interest" were dealt with entirely within the country, and within its own domestic legal framework, and related only to the State's own citizens and residents. However, the ever-increasing cooperation within the EU, also on matters such as health, welfare, migration, etc., means that there will also be increasing transnational (European-level) arrangements, and corresponding data flows, that will come under data protection law.

Guidance, in particular on what would be "suitable safeguards" in this regard, is therefore urgently needed to facilitate (upward) approximation of the data protection guarantees in these respects.

Criminal convictions: The laws in the Member States 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 their special rules on criminal convictions to data on other legal disputes or to data on "serious social problems" or indeed "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.

National Identity Number: There are also 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. These divergencies can have repercussions for the EU, if public bodies - or indeed private entities - were to start recording such numbers of foreign workers etc. Any attempt to allow for more data exchanges between public authorities (as are likely to be proposed in the new EU without "pillars") will also have to take these different rules and cultures into account.

4.6 THE RIGHTS OF DATA SUBJECTS

(a) The Rights Of Data Subjects In The Directive

The basic rights of data subjects contained in the Directive are not new: they were already contained in other international data protection instruments, such as the Council of Europe Convention No. 108, the OECD- and the UN Guidelines on data protection. These rights are:[133]

- the **right to confirmation** as to whether or not data relating to the data subject are being processed by a particular controller and, if so, to be given details of the processing (Art. 12(a), first indent, of the Directive);

- the **right of access to one's data**, including the right to be given a **copy** of the data in question, with "any available information as to their **source**" (Art. 12(a), second indent); and

- the **right to have the data rectified, erased or blocked** if they do not conform to the Directive, in particular, if they are incomplete or inaccurate (Art. 12(b).

The Directive adds to the latter, the right to have third-party recipients of subsequently corrected, erased or blocked data informed of the rectification, erasure or blocking, provided that this is not impossible or involves a "disproprotionate effort" (Art. 12(c).

Apart from these usual data subject rights, the Directive also stipulates a number of rights of data subjects that are novel or exceed those laid down in earlier international instruments, i.e.:

- a general **right to object** to the processing of one's personal data (Art. 14(a));

- a more specific **right to object to direct marketing** use of one's data (Art. 14(b)); and

- a new **right not to be subject to fully automated decisions** based on personality "profiles" (Art. 15), coupled with the right to be informed, on request, of the "**logic**" used in such decisions (Art. 12(a), third indent).

We must again limit ourselves here to a basic assessment of the level of convergence (or divergence) between the laws and practices of the Member States in these respects.

(b) The Rights Of Data Subjects In The National Laws

The right to confirmation, access and correction[134]

The laws in all the Member States studied 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 the law in Finland adds expressly that if controllers do not process data on the data subject they must inform him of that, too. 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, with some differences on certain specific matters. The most important difference in the laws is that some countries - in particular, 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], as the Directive says. 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. As the UK data protection authority has pointed out, this blanket exemption has no clear foundation in the Directive.

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 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 studied except Spain in principle give data subjects the right to obtain an actual 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 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 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] 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 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 branc h or department) which is approached must pass on the access request to other parts of the group as appropriate.

All the laws studied provide for the right of rectification or erasure and all of those except the Finnish law also expressly refer to "blocking " in this regard. 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). 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 in 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 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 ".

The general right to object

The general "right to object" to processing on "legitimate grounds" originates in France: it was included in the previous 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 studied 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 Irish law also limits the right to processing on the basis of these two criteria only. Indeed, the UK and Irish laws both add that the right can be exercised only on the ground that, for specified reasons, the processing causes (or is likely to cause) "substantial 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 - which would appear to be a considerably higher hurdle to overcome than is envisaged in the Directive, whih says that objections must be upheld if they are "justified".

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.

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. Thus, 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 applies it to all processing except processing necessary to fulfil a contract or pre-contract, and processing necesary to fulfil a legal obligation. As already noted, 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.

Under the French law, the right to object does not apply to processing in the public sector if the "regulation" regulating that processing contains a specific exemption to that effect (which confirms a narrow reading of the exemption under the previous law).

By contrast, the laws in Finland, Spain and Sweden do not provide for a general right to object at all, 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, under the heading the data protection criteria, in section 4.3. 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.

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.

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

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 offers the Member States two alternative ways of implementing this right. The first possibility is for Member States to stipulate that data data subjects have a right to object to direct marketing use of their data, and to ensure general publicity for this. Under the second, alternative option, data subjects must be specifically offered the right to object to direct marketing use of their data by controllers contemplating such use.

The situation in the Member States is in fact further complicated. First of all, several Member States, including 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 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.[135] The extension of the right to object to direct marketing-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 direct marketing use of their data and ensuring general publicity for this) is clearly chosen in just four of the countries studied: Austria (under separate legislation), the Netherlands, Ireland 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. 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 direct marketing 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) direct marketing use of one's data.

The second alternative option (under which data subjects must be specifically offered the right to object to the use of their data for such purposes) is similarly clearly chosen by some 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 several further countries – such as Finland, France, 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 studied 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. 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.[136]

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.

The right of data subjects not to be subjected to fully-automated decisions that "significantly affect" them

The provision in the Directive giving individuals the right not to be subjected to fully-automated decisions that have legal or (otherwise) "significant" effects for them stems from certain rules in the previous French law - expanded on in the new (amended) law in that country - which reflect the injunction in the law 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".

This provision in the Directive will gain considerable importance in the new socio-technical environment described in Working Paper No. 1, which is characterised by enormous increases in automated data collection (also from "things" relating to individuals, such as telephone- and mobile numbers, GPS data, or IP addresses), the ever-increasing linking of data to individuals (e.g., through face-recognition or automated car license plate readers), and the massive expansion in computing power and, hence, automated data linking and –analysis.

Following implementation of the Directive, the laws in all the Member States studied now contain provisions on the lines of the one in the Directive – but again with some significant differences. Thus, the laws in Austria, Belgium, Germany, Finland, the Netherlands, Portugal, Sweden and 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, Sweden and Ireland apply the exception relating to the data subject being allowed to "put his point of view" not only to contractual and 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 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.

Other laws 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. The right can be exercised "even when the other substantive conditions for provisional judicial protection" (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". There is to the best of our knowledge as yet no practice or case-law to show how this much broader provision will be applied.

The law in France retains and builds on two strict rules in the previous 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, by means of a notice 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 further discussed below.

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 of 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, and there is only very little national practice or national legal interpretation on this. The UK data protection authority (the Information Commissioner) feels that it is almost entirely limited to contractual or pre-contractual decisions (and feels that the whole provision 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.

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 France, which inspired the provision in the Directive, and where an in-principle prohibition has been in effect for many years, there was an investigation by the CNIL as long ago as 1991 which resulted in a system being abandoned through which insurance companies used automatic processing to exclude certain people from life insurance cover[137] – but there have been few, if any, cases since. The German authors Dammann and Simitis, in their Commentary on the Directive, 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.[138]

We feel that the best reading of the provision in the Directive is that it is indeed aimed at so-called expert systems, in which aspects of a person's personality or other somewhat intangible matters are evaluated – and not at the use of computers in more traditional processing of objective data, such as (say) Automatic Teller machines (ATMs or

"cashpoints") paying out, or not, depending on whether the person presenting a bankcard has enough money in the relevant account.

However, 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, at least on paper – but they still, in practice, rarely apply these rules in that way. 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.

Finally, we should note that the laws in all the Member States studied 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 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 law in Ireland extends 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". Portugal even extends the right 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. While this wording derives from the Directive, that instrument merely intended to give the Member States discretion in the matter. Merely repeating the words leaves the law unduly vague. These extensions are significant, given that the provision in the Directive on such decisions, read on its own, arguably applies to a very limited range of decisions only (as discussed above).

The reason we went into some detail on this issue is that, as explained in Working Paper No. 1, in the new socio-technical environment described there - that is, in the very near future - "smart" (expert) computer systems will be increasingly used in decision-making by both private- and public-sector agencies, including law enforcement agencies. Reliance on sophisticated computer-generated "profiles" (and in particular dynamically-generated profiles, in which the algoritm itself is amended by the computer as it "learns"), in any of these contexts, in our view undoubtedly fall within the scope of the provision.

This provision is therefore one that requires urgent elaboration and clarification, probably best first by the Article 29 Working Party, in the manner we recommend in our Final Report.

4.7 DATA SECURITY AND CONFIDENTIALITY

Note: We believe that one of the most important issues in relation to security and confidentiality is data breach notification. However, that is an issue dealt with in the e-Privacy Directive (Directive 2002/58/EC),[139] which is outside the scope of this paper. We must therefore limit ourselves to this note, stressing that this is an issue which will be increasingly important in the new socio-technical environment described in Working Part No. 1. We will return to this issue in our Final Report.

(a) Data Security And Confidentiality In The Directive

The issues of data security and confidentiality are addressed in Articles 16 and 17 of the Directive. Article 16 requires any person acting under the authority of the controller, including not just his own immediate staff but also processors (agents), to only process personal data as instructed by the controller (unless required by law to do otherwise). In both cases (own personnel or agent/processor), national law must stipulate 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.
>
> (Article 17(1))

For the agent/processor context, Article 17 reinforces this, first of all, by requiring the controller to only engage processors "providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out", and adding that the controller "must ensure compliance with those measures" (Art. 17(2)). Moreover, the processor's duty must be stipulated also in the "contract or [other] legal act" that governs the relationship between the controller and the processor (Art. 17(3)(1)), which must be in writing (Art. 17(3)(4)).

In practice, these stipulations mean that controllers should only employ personnel and agents that are properly trained and instructed, and subject to disciplinary or (in the case of agents) other contractual sanctions for any breach of this rule; and that both the controller and the processor must use appropriate technical and organisational security measures (with the security level depending on the issues listed in the second sub-clause of Article 17(1): technical state of the art; cost; risk level; and nature of the data).

The issues are related to the question of anonymisation/pseudonymisation and the risk of re-identification, discussed at some length in section 4.1, above. In particular, it may be recalled that the WP29 has made clear that if data are to be kept for a long period, the question of "state of the art" should be related to the probable technical capabilities at the future date when the data are still held: data must be protected against security risks (such as unintended re-identification) that are likely to arise in their "lifetime".

Finally, it may be noted that the Directive contains an exception to the normal rules on "appliable law" (discussed in Part 3, above), in that it says that controllers must *also* comply with their local legal requirements on data security (Art. 17(3)(2)). In other words, as far as data security and confidentiality is concerned, processors must comply *both* with the requirements of their own national law (the law of the place where they are established) *and* with the national law which applies to the processing as a whole (which will, as far as EU/EEA-based controllers are concerned, usually be the law of the country of establishment of the controller).

The issue of data security also ties in with the question of "privacy-enhancing technologies" (PETs), as noted with reference to German discussions in particular, in (b), below. We will return to PETs in more detail in our Final Report.

(b) Data Security And Confidentiality In The National Laws

The laws in all the Member States studied 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).
All the laws studied 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 of the laws studied 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 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.

The stipulation in the Directive, requiring controllers to comply with both their own national law and the law that is the "applicable" law in relation to the processing operations carried out on behalf of the controller, is repeated expressly in the Dutch law. The Finnish law, too, says that the processor must also comply with his local legal requirements (as well as with the security requirements of the country where his principal [the controller] is based).

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, adopted in 2001, therefore itself only refers to "appropriate" measures. However, even while considering this new law, the data protection authorities and –experts in Germany had been trying to clarify how data protection can be ensured in the "information era". A working paper produced at that time identified some new main aspects on which data protection should focus:[140]

- ✓ 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
- ✓ 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 further developed in a 2001 German expert report, *Modernisierung des Datenschutzrechts* (Mondernisation of Data Protection Law), commissioned by the German Ministery of the Interior.[141] Here, it will suffice to note that the working paper and this expert report already noted two matters of particular relevance to the present 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.

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. 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 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 is able to give such products its "seal of approval" (or to withhold such approbation).

At a different level, the Swedish data protection authority,as long ago as 1999, has issued a useful guide on how controllers and processors should approach data security measures, which it updated in November 2008.[142] 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.).

Overall, therefore, the basic, somewhat abstract requirements of the Directive concerning data security and –confidentiality are therefore not just generally re-stated in the laws of the Member States, but 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). Given that this is one area in which the practical requirements are largely common to all, irrespective of the details of the various 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 whatever instrument that might replace it) to European technical standards, in much the same way in which this matter is largely left to domestic industry standards in the UK.

4.8 TRANSBORDER DATA FLOWS (TBDFS)

(a) The Rules On TBDFs In The Directive[143]

The Directive deals with two types of transborder data flows: data flows within the EU/EEA, and transfers of data to non-EU/EEA (so-called "third") countries, and in the latter case distinguishes between third countries with, and without "adequate" data protection.

The basic rules are straight-forward: data flows within the EU/EEA should be unrestricted - provided that they relate to matters covered by the Directive, that is, by Community law (Article 1(2) of the Directive). The latter restriction on the "free movement of data" under the Directive is inherent in the fact that the Directive itself only applies (even now, for the time being, after the Lisbon Treaty) to matters within the scope of Community law and "in any case" not 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" (Article 3(2), first indent). That is not a technicality - on the contrary, the principle of free movement of data is predicated on the assumption that data protection is guaranteed (by the Directive) at a high level. The same is not (yet) guaranteed in what used to be the Third Pillar - and therefore, unless and until that is done, the principle of free movement of data can also not be extended into that area.

This is, indeed, one of the main challenges faced by the EU in terms of data protection. The "Third Pillar" Council Framework Decision on data protection in that area enshrines the principle of "availability", which suggests, if not complete, then still a high level of "free movement" of such data in relation to police and judicial cooperation[144] - but without effectively aligning data protection within the former Third Pillar with the fundamental-rights regime laid down by the Directive. The Stockholm Programme, too, contains fine words on ensuring a high level of data protection, across what used to be the three "pillars" - but without as yet clarifying how this should be achieved.[145] And that, of course, is the real challenge.

Data may also be freely transferred to third countries with "adequate" protection (if they are adequate in some respects, but not in others, provided the data fall within the adequately protected area) (Article 25(1)). And data may in principle not be transferred to third countries without adequate data protection (or to countries that are adequate in some respects,

but not in others, if the data fall within the not-adequately protected area), unless a special condition is met (Article 26(1)).

The problem here is that the process for making an finding of "adequacy" (or "inadequacy", although that is generally avoided) is long and tortuous. On the one hand, this is understandable: the EU should not too readily accept the "adequacy" of third-countries' laws or arrangements, or it will undermine its own data protection regime. On the other hand, as explained in the country reports on the Asian-Pacific countries in particular, the failure to engage with countries there in this respect has to some extent made them turn away from even trying to achieve EU recognition for their data protection regimes. There is a difficult balance to tread here.

(b) The Rules On TBDFs In The National Laws

Even leaving the complexities of relationships with third countries aside, even within the EU the issues are complex. Yet again, the relevant rules are not uniformly applied.

First of all, only a few States expressly provide for the free transfers of data within the EU/EEA; most imply this (by only imposing explicit restrictions on transfers to third countries) but do not spell it out. Of the few States that do stipulate this freedom, moreover, only one (Austria) makes clear that that freedom only applies with regard to processing within the scope of the Directive. This is of course essential, since there is no guarantee that processing that is outside the scope of the Directive - in particular, in the for now still-existing Third Pillar - is subject to adequate data protection (cf. Article 3(2), first indent, of the Directive). Yet most of the Member States studied fail to clarify this, at least explicitly. The uncritical appplication of the "free data zone"-rule in Article 1(2) of the Directive, so that it also places no obstacles in the way of Third-Pillar data transfers within the EU, is thus highly problematic and certain to lead to violations of data protection standards. Only if and when the three-pillar structure of the EU is abolished, and full and appropriate data protection ensured throughout all matters currently in those pillars (as discussed above, at (a)) - only then can a rule be adopted on the lines of Article 1(2), applicable to all data transfers within the EU/EEA, unlimited to matters within the scope of Community law. If the challenges of the new global-technical environment are to be met, that should happen sooner rather than later.

As concerns transfers of data to countries with "adequate" data protection, the main difference - but an important one - concerns the situation pending a formal finding of "adequacy" by the Commission. In Austria, Greece, Luxembourg, Portugal and Spain the law makes clear that in the absence of a Commission finding of "adequacy", only the national authorities can determine that a particular third countryprovides "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. By contrast, in some countries, like the UK, the assessment pending a Commission "finding" is left to controllers. This reflects a generally relaxed, limited-interference approach by the authorities there.[146] This would appear to be out of line with the views of the WP29, which acknowledged that "[t]he directive does not specify ... whether an authority should be charged with assessing the adequacy of data protection in third countries", but concludes from this that it is therefore at least "possible that national

legislation in Member States endows this task on national data protection authorities, whose authorisation may be required for the transfer of personal data to a third country to take place." Indeed, from the next paragraph, the WP29 would appear to feel that these are the only two real options:[147]

> Beside this possibility for national authorities to assess adequacy as allowed by national legislation, the Directive provides for Europe-wide decisions on adequacy to be adopted by the Commission, thus providing an added value of legal certainty and uniformity throughout the Community ...

The problem is that if one combines the basic "free transfers within the EU/EEA"-rule with the lax position in the UK (and some other countries), the strict rules in the first category of countries can be easily circumvented: the data protection authorities in these countries cannot (in terms of the Directive) stop transfers of personal data to the Member States with less strict rules, and the data can then be transferred from those other Member States to third countries in respect of which there is no formal "adequacy" finding, either at the EU level or by the authorities in the original country, on the basis that the controller feels that protection is nevertheless sufficiently ensured. We cannot assess how widespread this loophole is used (the basic impression is that compliance with the legal rules on data transfers is generally very low) - but a loophole clearly it is. What is more, in the new environment, in which data are constantly and routinely transferred to different jurisdictions, this problem - the use of this loophole, knowingly or unknowingly - will grow very fast.

Finally, there are divergencies in the application of the special conditions under which data may be sent to third countries without "adequate" data protection. It may suffice to merely note here that, yet again, the conditions are not uniformly applied: Some Member States 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 several others do not provide for the required derogation concerning transfers of data obtained from public registers. In this respect, the WP29 issued a working document specifically:[148]

> to address its concern that differing interpretations are made of the provisions of Article 26(1) in practice, which prevent these provisions from being uniformly applied in the different Member States.

It added that:

> TheWorking Party considers this document as an essential element of its policy on data transfers to third countries. This document should accordingly be read in conjunction with other work done by the Working Party in this domain, namely on "binding corporate rules", standard contractual clauses, and adequacy in third countries, including SafeHarbor.

The document gives guidance on the application of the various special conditions for data transfers to third countries without adequate protection, set out in Article 26(1) of the Directive. However, this has not led to real changes in the practice in the Member States studied. In particular, the "strict" countries noted above continue to subscribe, on paper, to the view that data should not be transferred from their jurisdiction to countries in respect of

which they (or the Commission) have not issued a finding of adequate protection; and the "laxer" countries continue to feel that the assessment can be left to controllers. Indeed, to the best of our knowledge, the "strict" countries do not ever issue any adequacy findings in respect of countries not already deemed adequate by the Commission.

Overall, in many Member States, whether strict or lax on paper, Article 26 therefore appears to be honoured more in the breach than through compliance. The only way to address this issue - which yet again will come to the fore in the new environment - is to have clearer guidance from the WP29, and a uniform policy of effective compliance in all Member States.

5. The difficulties in *enforcing* EU data protection law in the new technical global environment

The Directive contains various provisions aimed at ensuring the effective implementation and enforcability of the laws adopted to implement it. They fall into two broad categories: remedies that, according to the Directive, must be granted to individuals, i.e. procedures through which individuals (and in particular data subjects) can assert their rights and ensure that the law is adhered to in relation to the processing of personal data relating to them; and general enforcement powers that must be vested in the national data protection authorities (DPAs) that must be created under the terms of the Directive. In this section, we will first briefly look at the remedies for individuals envisaged in the Directive: judicial remedies, including the right to compensation; and the right to complain to the data protection authorities. After that, we will, equally briefly, examine the role, status and powers of the DPAs. In each case, as before, we will first look at the relevant requirements laid down in the Directive, and then at the way in which these are implemented in the national laws. As usual, we will include some critical assessments of these matters as appropriate.

We note that the issues addressed here are also the subject of a separate, extensive report, on a Comparative Legal Study on assessment of data protection measures and relevant institutions, commissioned by the EU's Fundamental Rights Agency (FRA).[149] We defer to that study for more comprehensive detail on the above matters. Indeed, we have felt that because this matter is addressed in such detail in the other study, we could deal with these issues somewhat more briefly, partly again with reference to earlier studies. However, we believe that our assessments - in particular, our conclusions about the inadequacies of some of the remedies and powers, but in particular also about the relative weakness of the enforcement system in practice - still stand, and will be confirmed by the more targetted FRA study.

5.1 INDIVIDUAL REMEDIES

THE RIGHTS TO A JUDICIAL REMEDY AND COMPENSATION

(a) The Right To A Judicial Remedy And The Right To Compensation Envisaged In The Directive:

Articles 22 and 23 of the Framework Directive stipulates that Member States must provide the following remedies to each individual:

> a right to a judicial remedy for any breach of the rights guaranteed to the individual by the national law applicable to the processing in question; and

> a right to compensation for any damage suffered by the individual as a result of an unlawful processing operation, or of any other act incompatible with the applicable national law.

The two rights are here discussed together, because the right to compensation is typically one of the remedies that individuals can obtain from the courts.

This first provision echoes Article 13 of the European Convention on Human Rights which stipulates that:

> Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority ...

Article 13 ECHR has been held to require, first of all, (speedy) access to an appropriate forum, and secondly, the right of such a forum to rule on the merits of the issue in question and the power to order remedial action. It has also been held that this forum should "preferably" be a judicial one.[150] The Directive goes beyond this by stipulating that the forum must always be judicial.

Article 22 adds that the requirement of a judicial remedy is "without prejudice to any administrative remedy for which provision may be made, *inter alia* before the supervisory authority referred to in Art. 28" (as further discussed under the heading "*Complaints To The Data Protection Authorities*", below).

There is no specific guidance in the Directive on the precise form (or forms) that the remedy should take (other than that the forum should be a judicial one), and the Working Party too has not addressed this issue to date. However, in this respect it is instructive to look at the clarification issued by the EU on the somewhat weaker but still similar requirement in the "Safe Harbor" principle on enforcement, that there must be an "independent recourse mechanism" available to data subjects. In the Frequently Asked Questions (FAQs) on this principle, it is made clear that the mechanism must be able, in so far as feasible, to "reverse or correct" any effects of non-compliance, to ensure that future processing will be in conformity with the Safe Harbor principles, and where appropriate, that processing of the personal data of the individual who has brought the complaint will cease (FAQ 11). Clearly, *mutatis mutandis* these should also be the minimum requirements for effective judicial remedies under the Directive. They imply that courts, apart from awarding compensation, should also be able to issue injunctions in the relevant proceedings, ordering controller to either take specific action or to refrain from certain matters (injunctions are indeed expressly mentioned in Safe Harbor FAQ 11).

The right to a judicial remedy is granted to individual data subjects; under the Directive, there is no right to "class actions" before the courts, although the Member States may, of course, provide for them if this fits in with their general system of law.

It should be noted that Article 22 expressly stipulates that the rights which data subjects enjoy are those of "the national law applicable." As explained in Part 3, especially within the EU, this can be the law of a different State than the country of nationality or residence of the data subject. At least within the EU, the rights of such data subjects (and for that matter the exceptions and derogations from those rights as also described in that sub-section) are

therefore to be determined by reference to the place of establishment of the controller rather than by reference to the place where the data subjects live, or where their data are collected or otherwise processed.

Presumably, the right to compensation under Article 23, too, is to be granted under the "applicable law". This too is important, because, as we shall see at (b), below, the laws in the Member States differ in this respect. However, it would seem that (at least in the opinion of the Article 29 Working Party) States are not entirely free to determine what kind of damage may provide a cause of action. This is again made clear in an assesment of the appropriateness of safeguards in the context of transborder data flows, specifically in its comments on the adequacy of sectoral codes of conduct in this regard. On this, the Working party writes that:[151]

> If the self-regulatory code is shown to have been breached, a remedy should be available to the data subject. This remedy must put right the problem (e.g. correct or delete any inaccurate data, ensure that processing for incompatible purposes ceases) and, if damage to the data subject has resulted, allow for the payment of appropriate compensation. **It should be borne in mind that "damage" in the sense of the data protection directive includes not only physical damage and financial loss, but also any psychological or moral harm caused (known as "distress" under UK and US law).** (emphasis added)

If this applies in that context, it should also apply to the implementation of the right to compensation in the national laws of the Member States.

However, the question of "applicable law" is, also in this regard, separate from the issue of forum. As the Belgian law makes clear, the courts of EU Member States may be called upon, in this respect and more generally, to apply and enforce the law of another EU Member State, if that law of that other State is the "applicable" law in respect of the processing in question. Most other laws do not deal with this issue, or leave it to the general principles of their legal system to determine the forum in this respect, but the principle set out in the Belgian law would still appear to be the most appropriate one: without it, data subjects would have to resort to foreign fora, which would be prohibitive.

Even so, this may be problematic, in the same way as in other respects already mentioned, i.e., if a foreign "applicable" law were to provide less rights, or wider exceptions, than are provided for in the domestic law of the country concerned, and if that wider protection were to be regarded as a constitutional requirement in the data subject's home country. Many national courts would, in such circumstances, refuse to apply the (from their constitutional point of view, deficient) foreign law, because to apply it would breach their domestic *ordre public*. We will look further at this at (b).

(b) Judicial Remedies And Compensation In The National Laws:

All the Member States allow for the possibility of data subjects seeking redress, and corrective action, though the courts. This includes both the possibility for individuals (i.e. data subjects) to obtain damages by means of court action, and the possibility to obtain mandatory or prohibitive injunctions (the former order a defendant to do something; the latter to refrain from doing something, or to stop doing it).

In most States, the questions of how and when remedies such as injunctions, or damages, are to be awarded are left to the ordinary law on (administrative or civil) liability. At most, in some countries in which there is not a general basis for such liability (such as the French *faut*, the German *unerlaubte Handlung*, and the Dutch *onrechtmatige daad*), the data protection law creates such a special head (or tort), or such a special basis for liability is added to the more general laws in that regard. Similarly, subject to a comment about transnational proceedings, made later, it suffices to note that the questions of forum and procedure are also everywhere basically determined by the ordinary procedural laws (i.e., the laws on administrative or civil procedure). This also means that, normally, the domestic courts of the Member States will assume jurisdiction over actions by foreign controllers that are alleged to have caused damage or distress to claimants who are nationals or permanent residents of the State to which the court pertains.

However, as already noted (but as is not always clearly spelled out in the national laws, with the notable exception of Belgium), under the "applicable law" rules in the Directive and (more importantly) in the relevant national law, these domestic courts may have to apply the law of the controller to the substance of the issue.

In principle, in respect of damages, this may not cause too many problems, even though there are some differences in the basis for liability in the different Member States, and in particular in respect of the terms that may relieve a controller of liability. 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 the civil code. In Finland, France and Luxembourg, too, the ordinary rules on civil- and administrative liability apply. In Ireland, the law (in effect) makes any breach of the data protection 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 actual (pecuniary) 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: immaterial damage can only be awarded if material damage has been proven.

Under the relevant international instruments on private international law (conflict of law), at least within the EU, the domestic courts are likely to respect such restrictions on liabilities in "applicable" foreign laws. A Dutch court will, therefore, probably only award compensation over data protection issues to a Dutch national, against a controller in the UK, if the Dutch

claimant suffered at least also material loss. In such a case, decided by a Dutch court but applying UK law, the court would refuse to award compensation for immaterial damages in the absence of material damages (even though, if the case had to be decided on the basis of Dutch law, against a Dutch controller, the court could have awarded compensation for immaterial damages alone, even in the absence of material damages).

However, as already noted at (a), the courts in a number of countries are less likely to accept this application of a foreign law when it comes to the actual violation of data protection principles, and when the claimant is seeking not damages (or not only damages) but (also) injunctive relief. This will be especially the case if the issue touches directly on the constitutional "core" of the right to privacy or informational self-determination, or on another constiutional right, such as freedom of expression and freedom to seek, receive and impart information without interference by public authorities and regardless of borders (as discussed in section 2.3, above).

We believe that if an issue came before the courts in (say) Germany (or Spain, or Italy) in which, on the basis of the "applicable law" rules, a foreign law (say, the UK Data Protection Act) applied, and if that law failed (from the domestic point of view of the court) to adequately protect such a constitutional right, the domestic court would refuse to give effect to the foreign law - and thus to the "applicable law" rules in the Directive. Specifically, especialy also in the light of other rulings on transnational matters - such as rulings by courts in Germany, France and elsewhere on the sale of Nazi memorabilia over the Internet or on holocaust denial websites - it would not be suprising if courts in EU Member States were to issue mandatory or prohibitive injunctions against foreign controllers, including controllers in other EU Member States, in order to protect the constitutional rights of their own citizens.

We do not believe that this question has yet arisen anywhere in the EU. However, in view of the ever-expanding generation, dissemination and other processing of personal data, in an increasingly frontierless world (as described in Working Paper No. 1), this is an issue that will inevitably arise. Any review of the Directive must address it, and we will make further comments and suggestions on the issue in our Final Report.

Indeed, and we may end this sub-section on this, it appears that litigation in the courts by ordinary citizens is extremely rare. In the UK, the case of Naomi Campbell, briefly set out in section 2.3(b), above, was the first case ever in which compensation was awarded over breaches of data protection law, but remains a very rare case. In other countries there may be more actions, but in most, the cost and effort of formal court proceedings deter most potential claimants.

In our Final Report, we will examine if this can be and ought to change. We believe that, especially in the light of the weakness of enforcement by the data protection authorities (as noted in the next sub-sections), possibilities for empowering ordinary citizens should be further explored. We will examine why class actions are still extremely rare in Europe, also on data protection issues, and whether other, non-EU countries have more effective systems of this kind in place (or whether more unusual laws such as the *Qui tam* laws in the USA could provide useful examples).[152]

THE RIGHT TO COMPLAIN TO THE NATIONAL DATA PROTECTION AUTHORITY

(a) The Right To Complain As Envisaged In The Directive:

The Directive requires Member States to give their data protection authorities the power to receive "claims" - essentially, complaints - from data subjects. As it is put in Art. 28(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.

The right in the first sub-paragraph must be distinguished from the right in the second subparagraph: they differ in scope and effect.

The right laid down in the first paragraph is very wide: it allows any person to lodge claims concerning "the protection of his rights and freedoms in regard to the processing of personal data." In other words, these claims need not relate to specific rights of data subjects (like the judicial remedy of Art. 22) nor, indeed, to any particular provision of the national law implementing the Directive (like the right to compensation of Art. 23). People must be able to lodge complaints based on the wider and, in certain countries, constitutionally enshrined right to data protection by reference to a general right, such as the right to "informational self-determination" derived from the proto-right of "respect for one's personality" (as in Germany) or to the need to protect "human identity" in respect of the processing of personal data (France), or at least as enshrined in Article 8 ECHR.

Also of interest is the fact that such claims may be lodged, not just by the individual himself, but also by "an association representing that person." This does not quite amount to "class actions", but its effect may be similar: the Directive clearly envisages certain organisations such as civil liberty organisations, consumer associations, trade unions or indeed specialised data protection action groups taking up cases of individuals or groups of individuals to test the law and expects the data protection authorities to accepts such claims.

While the Directive does not spell this out in so many words, clearly the national data protection authorities are expected to act upon such claims. They would to that end need to establish the facts by contacting the controller. If appropriate, they can use their general powers of investigation, including their right of access to data being processed and to premises, etc., used in such processing, as further discussed at 5.2. What action they can, or should, take on the basis of their investigations is however left somewhat unclear in the Directive, and will depend on the general "powers of intervention" granted to them under the national law, as again further discussed at 5.2. In some countries, they may be empowered to order the correction, blocking, erasure or destruction of data; in others they may only be able to deliver "opinions" (cf Art. 28(3), second indent, of the Directive). In all Member States

they should however be able to "engage in legal proceedings." In other words, they should be able to either themselves prosecute controllers who have violated the law and/or who refuse to comply with such orders or opinions, or to pass on the file to the general prosecuting authorities (Art. 28(3), third indent, of the Framework Directive).

The right in the second sub-paragraph of Art. 28(4) of the Framework Directive is somewhat different. First of all, it is narrower than the right in the first sub- aragraph. It concerns not the testing of processing against a broad concept of data protection but the much more limited assessment of the "lawfulness" of processing with regard to which the controller invokes an exception, exemption or derogation, as provided for in Art. 13, i.e. relating the national security, defence, or criminal investigations, etc.. The relevant data protection authority[153] must carry out a "check" when a claim to that effect (i.e., a request for such an assessment) is made. In other words, it must investigate (a) whether Art. 13 applies, in general or in the particular case, and (b) whether, if and to the extent that Art. 13 can be relied on in principle, it has been applied correctly in the case at hand.

It should be noted that if the authority concludes that Art. 13 cannot be invoked in the particular case, the check must be proceeded with under the first sub-paragraph, and the complainant must be "informed of the outcome" of the investigation. In other words, he must be told that Art. 13 did not apply, and he must be told what remedial action has been taken.

However, if the authority finds that Art. 13 can be invoked, the complainant need only be told "that a check has taken place." He need not be told what the check revealed, whether this required any remedial action, or what the authority has done to ensure that that action is taken.

On the other hand, it is interesting that the "claim for a check" on whether reliance on an exception, exemption or derogation is lawful can apparently be lodged, not just by a person whose rights are directly affected by such exceptional processing, but by "any person."

The point to be made is that, on the one hand, the right to lodge claims is very wide and can provide for quick, cheap and informal redress. In that sense the right to lodge claims is to be preferred to the judicial remedy of Art. 22 and/or the lodging of claims for compensation. However, on the other hand, the standing of the individual in such proceedings is rather weak. He can complain and may expect his complaint to be investigated by the data protection authority. However, he is not, by the Directive, granted any procedural rights or the right to be involved in the investigation. With regard to ordinary complaints, the data subject is merely entitled to be "informed of the outcome" of this process. If his complaint concerned the application of an exception, exemption or derogation, he may not even be informed of that: all that he must be told is that "a check has taken place."

It is, therefore, important that the Directive stipulates that the complaints procedure before the national data protection authority is without prejudice to the right of data subjects to a judicial remedy. The information provided to complainants (in effect, the rulings of the national data protection authorities on individual complaints) must therefore at least be subject to judicial review; and (in the light also of the ECHR) such reviews should deal with the substance of individual complaints and not merely with the formal propriety of the authority's investigation.

(b) The Right To Complain In The National Laws, As Exercised In Practice

The right to complain to the data protection authorities, and the responses of those authorities to such complaints, must be seen in the context of the general exercise of the powers vested in those authorities, as discussed below, at 5.2(b). Here, it may suffice to note that the effectiveness of this system largely depends on three factors: the formal powers that the authorities have to act on the basis of a complaint; their willingness to take forceful action on behalf of data subjects, against controllers - which in turn very much depends on how they see themselves, as discussed below, and further at 5(2)(b); and resources. In many ways, the first factor is almost the least important (although without formal powers, DPAs will be unable to act strongly even if they wanted to: such powers are thus a necessary pre-condition for proper assistance to data subject, but not a sufficient condition).

In practice, as shown in several studies, with some notable exceptions, many data protection authorities tend to see themselves more as conciliators or mediators than as fierce watchdogs or privacy advocates: they prefer to find an "amicable" solution to conflicts between data subjects and controllers, to fighting battles on issues of principle. Enforcement is weak, both generally (as discussed at 5.2(b)), and in the context of investigations of individual complaints.[154] This can be partly explained by the DPA's somewhat confusing roles (as discussed at 5.2(a)), and partly by a serious lack of resources - but it is still frustrating for data subjects.

The situation in the UK is perhaps worse than in most other countries, but is still illustrative of the problems. A recent study found, on the basis of the figures of the Information Commissioner's Office (ICO) itself, that whenever possible, cases were dealt with through "advice and guidance", without actually even examining whether the law had been violated. Only cases that, in the view of the ICO, raised wider issues or showed serious, persistent violations, were pursued at all (which is little comfort for data subjects whose complaints are deemed not serious enough, or incidental).[155]

Serious enforcement action was only taken in a minute part of even those cases in which the ICO found that the law had "probably" been broken (a reported total of 3,600 in 2006-07, but this does not include the vast numbers of cases dealt with without even checking if the law had been complied with). In some 36 cases, including some well-publicised cases concerning banks, the controllers formally promised to behave in future, and that ended the matter. Actual enforcement action on the basis of complaints (or indeed otherwise) is rare. Thus, so-called "Enforcement Notices" (effectively, orders issued by the ICO to controllers) were issued in only about 25 cases between December 2006 and December 2008, all relating (only) to manifest abuses highlighted by 'many' or 'hundreds' of complainants (most relating to unsolicited telemarketing calls). Prosecutions are brought in only the rarest of cases: in 2006 - 07, there were only about 11 prosecutions, in eight cases, relating to just a few fairly obvious issues (such as illegal telemarketing or selling of police data).[156]

What is more, it appears that individual complainants are not, or barely, or rarely, involved in the process leading to the resolution of their complaints, and are not asked if they are satisfied with the resolution (either before or after it is formalised).

A more general problem, not limited to the UK, is that the authorities' approach to dealing with complaints may give the impression of 'soft' and negotiable enforcement of the law, which is not conducive to wider compliance and may in part account for the widespread disregard, in many countries, for the law. The absence of readily accessible comprehensive information on how the law is enforced in individual cases is a serious problem: many DPAs publish selected case summaries or general guidance on their websites or in their annual reports, but in many countries it is difficult to get a precise view of exactly how the law is applied in each and every respect (Germany is an exception here, with extensive reports and dedicated academic and practitioners' journals examing DPA rulings from the various data protection authorities in detail).

5.2 STATUS AND POWERS OF THE DATA PROTECTION AUTHORITIES

(a) The Status And Powers Of The DPAs As Envisaged In The Directive:

The Directive stipulates that each Member State must appoint "one or more" data protection authority (this allows for special authorities to supervise special matters, such as processing of personal data by the police or the security services, and for different authorities to supervise data processing in different states belonging to federal countries such as Germany) (Article 28(1)).

status

Crucially, the Directive stipulates that these authorities must be given a status and facilities that ensures that they can "act with complete independence in exercising the functions entrusted to them" (*idem*).[157]

general powers

They must moreover be provided with "investigative powers" (such as powers of access to data and processing operations), "effective powers of intervention" (including powers to issue orders to, e.g., block, erase or destroy data) and "powers to engage in legal proceedings" (Article 28(3)). They must also, as already noted, be able to investigate complaints ("check claims") from data subjects and organisations representing them (Article 28(4)). And the DPAs in the EU must be able to cooperate with each other, and exercise their powers on each other's behalf (in the investigation of international complaints, e.g., from a data subject in one country against a controller in another) (Article 28(6)).

Particularly important are the powers to demand access to all data "forming the subject matter of processing operations" and to all other information "necessary for the performance of its supervisory duties" (Art. 28(3), first indent, of the Framework Directive). Until the adoption of the Directive, this power had been lacking in some countries, such as the UK.

The Directive is somewhat ambiguous about the "effective powers of intervention" that must be granted to the DPAs; it would appear that the Member States can choose among the various powers listed and can therefore either rely on "opinions" or "warnings" that (while usually followed) are not formally binding, or on more formal "directions" or "notices" that

are binding. However, the text of the Directive does make clear that, whatever powers are granted, they must be "effective." Dammann and Simitis believe that non-binding "opinions" and "warnings" can suffice with regard to public-sector data users, but that for the private sector the supervisory authorities must be able to resort to binding measures if less formal interventions fail to have the desired effect.[158]

The provision on the power "to engage in legal proceedings" furthermore allows the Member States to either give the national authorities themselves the power to prosecute persons or organisations suspected of having violated the law or to allow them to report ("denounce") suspected violations to the prosecuting authorities.

All in all, on paper, the DPAs must therefore be given quite wide-ranging powers (although some clarification, especially on the "effective powers of intervention", would still be useful).

audits and "prior checks"

One particular power that is not mentioned in the Directive, but that many DPAs find very useful, is the power to carry out "data protection audits" of processing operations, or the totality of operations by certain controllers (in the public and private sector), to verify if those operations meet the requirements of the law.

A further power, mentioned in connection with notification, in Article 20, is the power of the DPAs to carry out so-called "prior checks", on processing operations that are "likely to present specific risks to the rights and freedoms of the data subjects". The idea is based on the system of "prior opinions" (*avis préalable*), which already existed in France under the 1978 law predating the Directive.

The Framework Directive does not clarify what kinds of processing operations are to be considered "risky" and thus covered by this requirement. Instead, it leaves them to be determined by the Member States; see Art. 20(1). However, Preamble 53 clarifies that:

> certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of *excluding individuals from a right or benefit or a contract*, or *by virtue of the specific use of new technologies*. . . . " (Emphasis added.)

The use of "sensitive data" in a processing operation may also generally be seen as indicative of the existence of a "specific risk." In other words, the Directive suggests that the requirement of a "prior check" would be appropriate with regard to the processing of "sensitive data" and with regard to what could be called "sensitive processing," such as processing involving the use of a national identification number or other "identifier of national application" or processing involving the taking of (fully) "automated decisions".

The Directive is also not very clear about the implications of such "prior checks," except that it seems clear from the very word "prior", that processing subject to such a check may not take place until such a check has taken place. It is therefore again left to the Member States to determine what the consequences of such a check will be. As it is put in Preamble (54) to the Framework Directive:

> the supervisory authority may, according to its national law, give an opinion *or* an authorization regarding the processing. . . . (Emphasis added.)

In practice, as shown below, at (b), the systems adopted by the EU Member States vary considerably.

However, we believe that the idea of "prior checks" - albeit in a new form, with much earlier and more technical input from the DPAs (who would need to be equipped for the latter), could be a very useful tool in the new global technical environment described in Working Paper No. 1. We will return to this in our Final Report.

(b) The Status And Powers Of The DPAs In The National Laws, As Granted And As Exercised In Practice:

status

The laws in most Member States stipulates, in accordance with the Directive, that the national DPA "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) 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*. Processing by private-sector controllers (although subject to unified substantive rules in the federal data protection law) is often still supervised by authorities that are part of a local government or ministry, but this is being changed to achieve (belated) compliance with the Directive.

Overall, the picture is therefore rather mixed,[159] and much could still be done to really ensure full independence and freedom from influence for the DPAs. However, that is only part of the picture; as much depends on the powers they are given and, especially, on the authorities' willingness to use them.

general functions and powers, and their use in practice

Data protection authorities are rather odd "beasts": they combine a number of functions that may seem - indeed are - in part conflicting. Thus, in all Member States,

- 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.

The advice provided in the first role - 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 precondition: although in theory a "negative opinion" can be overruled by reference to the *Conseil d'État*, this avenue has rarely, if ever, 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 "caselaw" 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, banking, 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, such as "personal data"). 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.

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 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 – tend to be extensive, detailed and in-depth. All aspects of the processing operations in question are looked at and discussed with the data controllers (less so with representatives of data subjects), and precise and detailed views and opinions expressed on how the law is to be applied to them.

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.

In most countries, if they believe that matters are amiss, the DPAs may order remedial action - usually subject to an appeal to a court or (in the UK) 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 DPAs 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 it is put in the UK data protection authority's main policy document:

> We will put in place systems to ensure that Regulatory Action we take is in proportion to the harm or potential harm done. We will not resort to formal action where we are satisfied that the risk can be addressed by negotiation or other less formal means.

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 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 tend to 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. This impression is reinforced if such "negotiated solutions" are unreported: many DPAs regard publicity about investigative and enforcement action as something to be reserved for particularly serious cases, in which the contoller was uncooperative. But this means that the basis for "solutions" reached with "cooperative" controllers remains hidden (sometimes even to complainants who started the process).

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".

As already noted, 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 indeed only have to be "reminded" by the authority of his duty to allow such access.

Other cases however are more complex, and in those the DPAs often try to reach a compromise acceptable to it (the DPA) and the controller - but often without consulting or involving the data subject (and indeed sometimes without even informing the data subject of the outcome, as is required under the Directive).

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 straightforward 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.

When there is no compromise, no negotiated solution, 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 issue so-called 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.

However, as will be clear from the above, 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 cases (including cases exposing quite manifest breaches of the law) are dealt with through the above-mentioned discussions and negotiations.

Everywhere, criminal prosecutions are similarly extremely rare, even for obvious offences such as non-registration. In the UK, it is not unreasonable to believe that the vast majority of the 2.3 million registered (and actively trading) companies should be registered, but only about 12% is - which means that hundreds of thousands are breaking the law. One could find similar figures elsewhere.

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 the DPAs (and more in particular the power to carry out "audits") in the "Dublin Workshop" (held in April 2002), which concluded (as will also be clear from the above) that there were 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 felt that they should seek to agree protocols and procedures for mutual cooperation, on the basis of a clear understanding of each others powers (and limitations).

In view of the fact that, in the new global technical environment described in Working Paper No. 1, there will be evermore cross-border processing (and transfers) of personal data, this is an issue of increasing importance, and we will return to it in our Final Report.

Here, we may end this brief overview of the powers and actions of the DPAs with the rather sombering conclusion, that the main powers vested in the DPAs, as currently used, have not been able to counter continuing widespread disregard for the data protection laws in the Member States.

"Prior checks", audits and seals

Some authorities and activists have placed some hope in relatively new, or at least to date under-used powers, or powers which are only effectively used in some countries. First mention should be made of the system of "prior checks", envisaged by the Directive, but the implementation of which is almost entirely left to the Member States.

The system is most widely developed in France, where 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 has generally felt that no such checks should be introduced for any processing (although there has recently been some discussion of the possible need for such checks in relation to DNA databases and a national ID register).

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. In some countries, a prior check is required for all processing of sensitive data, or for all "interconnections" between different databases, or for processing by credit reference agencies; in some for the taking of fully automated decisions; etc.[160]

The main point to note, however, is that these requirements have (outside France) tended to become fairly bureaucratic formalities (if they are complied with at all). At most, they have resulted in certain controllers, such as private detective in the Netherlands, at least applying for the check, for fear of loosing their license (although doubts remain over the extent to which such firms complied with the more substantive requirements of the law). 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 feels that the system 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.

A major problem with "prior checks", even in countries such as France, is that the "check" is still usually only performed on systems that have effectively already been "cast in concrete": the DPA can often, at best, try to tinker with some minor details of the system; it is usually much to late to re-think systems fundamentally. A further problem is that many DPAs lack the kind of highly computer-skilled and information-policy-trained staff that is needed to really thoroughly review a proposed database or computer system.

We nevertheless feel that the system holds promise, and - if these defects could be addressed - could provide a model for tackling some of the challenges noted in Paper No.1 and in the present paper. We will therefore return to this in our Final report.

In the Netherlands, the authorities have for some years carried out detailed "privacy audits" of selected controllers, in order to enforce the law. This is also possible in Ireland, 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.

This too is a measure that could be further encouraged, both on a voluntary basis, by companies and organisations that wish to be seen to be acting fully in compliance with the law, and as an enforced measure, against those who are suspected of systematic breaches of the law (or where at least systemic problems are suspected).

One problem with both audits and "prior checks" carried out by the DPAs, is that they are very time- and person-power-consuming, and can therefore only ever be applied in relatively rare cases. An alternative has recently been established in the form of the "European Privacy Seal" or *EuroPriSe*, which is modelled on the data protection seal system of the German *Land* of Schleswig-Holstein. This system (unlike previous, purely-private initiatives) is centred on the issuing of the seals by cooperating data protection authorities (acting as certification bodies), working with specially-trained and accredited experts.

It is too early to assess the effectiveness of the European seal, or the level of up-take. However, one matter that would greatly contribute to that would be the system enshrined in the Schleswig Holstein data protection law, which allows public authorities to give preference in their purchases of computer hard- and software that have obtained the local seal. This too is a system that could be further examined at a European level. We will therefore come back to that suggestion in our Final Report too.

- o –O – o -

NOTES TO WORKING PAPER NO. 2:

[1] We are submitting separately, five reports on the data protection laws in the countries on which we agreed to focus, i.e., Denmark, France, Germany, the UK, and the Czech Republic. This paper also draws on, and in parts repeats, sections from earlier work by the author, and in particular, as far as the Directive is concerned: D Korff, Data Protection Law in Practice in the European Union, FEDMA (Brussels) / DMA (New York), 2005; and as far as the national laws are concerned: D Korff, Comparative Summary of National Laws, University of Essex / European Commission, 2002, and the *Country Reports* prepared in connection with the FEDMA/DMA book, just mentioned. The information in these earlier reports has been updated when possible from information in our possession, in particular in relation to the focus countries, but cannot provide a comprehensively updated view on all the laws in all the 27 EU Member States (plus the EEA States). Where the report refers to "the laws in all the Member States studied" (or similar), this therefore specifically includes the laws of the five focus countries, with additional information from the somewhat older reports just mentioned.

[2] Cf., at the European level, the following documents issued by the "Article 29 Working Party" (hereafter such documents are referred to simply by "WP" and their number): WP67, Working Document on the Processing of Personal Data by means of Video Surveillance, 25.11.2002, WP89, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 11.02.2004. An example of (strict) regulation at the national level can be found in the Directive on Closed Circuit Television Systems, issued by the Greek data protection authority on 26.09.2000 (Reference No. 1122).

[3] WP105, Working document on data protection issues related to RFID technology, 19.01.2005, WP111, Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology, 28.06.2005. Cf. also the comments on data contained in an RFID chip in WP 136, Opinion Nº 4/2007 on the concept of personal data, 20.06.2007.

[4] WP80, Working document on biometrics, 01.08.2003, WP96, Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system

on visas (VIS), 11.08.2004, WP112, Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 30.09.2005. Cf. also the comments on biometric data and DNA in WP 136, Opinion Nº 4/2007 on the concept of personal data, 20.06.2007, with reference to Council of Europe Recommendation No. R (2006) 4 of the Committee of Ministers to Member States on research on biological materials of human origin, of 15.03.2006.

[5] WP58, Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPV6, 30.05.2002, WP69, Opinion 1/2003 on the storage of traffic data for billing purposes, 29.01.2003, WP115, Opinion 5/2005 on the use of location data with a view to providing value-added services, 25.11.2005.

[6] WP05, Recommendation 2/97: Report and Guidance by the International Working Group on Data Protection in Telecommunications ("Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet"), 03.12.1997, WP06, Recommendation 3/97: Anonymity on the Internet, 03.12.1997, WP16, Working Document: Processing of Personal Data on the Internet, 23.02.1999, WP17, Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, 23.02.1999, WP28, Opinion 1/2000 on certain data protection aspects of electronic commerce,03.02.2000, WP37, Working document "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection, 21.11.2000, WP43, Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union,17.05.2001, WP56, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 30.05.2002, WP60, Working document - First orientations of the Article 29 Working Party concerning on-line authentication services, 02.07.2002, WP68, Working Document on on-line authentication services, 29.01.2003, WP118, Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services, 21.02.2006. For an overview and discussion of the earlier documents, see D Korff, European data protection law & the Internet: a briefing on the Opinions and Recommendations of the Working Party established under Art. 29 of the EC Directive on data protection, relevant to the collecting, storing, dissemination and use of personal data on the Internet, prepared for the Privacy Leadership Initiative, December 2000.

[7] We will therefore not examine the limitation of the applicability of the Directive to data held in automated files and in "structured [manual] files" only, nor the (in itself quite important and complex issue) of the non-applicability of the Directive to "legal persons" or deceased persons. Also not discussed here are the (again nevertheless important) issues of the special exception under Article 8(4) relating to "substantial public interest", and the relationship between data protection and freedom of information law (FOI). For a discussion of these matters as addressed in the national laws, see D Korff, Comparative Summary of National Laws (footnote 1, above), sections 3.1 (structured files), 3.2 (deceased and legal persons), 7.4 (subtantial public interests) and 10.2 (FOI).

[8] The "Pillar" structure of the EU was abolished by the Lisbon Treaty, which came into force in December 2009, i.e. shortly after the formal end of the present study, but before the final revision of this paper and the Final Report on the study. However, neither the EC- and EU legal instruments - including the Directive - nor the national laws have yet been brought into line with the new legal situation; the Lisbon Treaty allows for a transitional period. The descriptions in the present paper of the laws relating to former First- and Third-Pillar issue are therefore still correct at the time of writing. Indeed, this study is envisaged as a basis on which to review the data protection regime in the EU (including the data protection directives), also in the light of the Lisbon Treaty. . In view of the transitional situation, in this final, revised version of this paper, references to the "pillars" have often been qualified by such wording as "the (former) Third Pillar" or "what used to be the First Pillar". However, given that the various instruments - and the data protection directives in particular - for the time being continue to apply as before, this has not been done rigorously.

[9] For summaries of the relevant case-law of the ECtHR and the ECJ, see D Korff, *Paper No.4: The Legal Framework*, in: I Brown & D Korff, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2004. Subsequent cases have, if anything, further reinforced this data protection-friendly jurisprudence.

[10] See D Korff, The feasibility of a seamless system of data protection rules for the European Union, Study for the European Commission, 1998.

[11] For a brief but critical overview, see the "Issue Paper" by the Council of Europe Commissioner for Human Rights, Thomas Hammarberg, on Protection the right to privacy in the fight against terrorism, Strasbourg, December 2008. The author of the present paper assisted in the drafting of this paper.

[12] See D Korff, The feasibility of a seamless system of data protection rules for the European Union, footnote 9, above.

[13] D Korff, The feasibility of a seamless system of data protection rules for the European Union (footnote 10, above), Conclusions.
[14] For a quite detailed overview of these limitations, exceptions and exemptions in the laws in the then EU15, see D Korff, Comparative Summary of National Laws (footnote 1, above), section 10.3.
[15] *Idem*.
[16] COE Recommendation R(87)15 of the Committee of Ministers to Member States, Regulating the Use of Personal Data in the Police Sector (1987)
[17] Article 29 Working Party Opinion on online social networking (Opinion 5/2009 of 12 June 2009). The Opinion draws on earlier papers, including: the Berlin International Working Group on Data Protection in Telecommunications' Rome Memorandum of March 2008; the 30th International Conference of Data Protection and Privacy Commissioners' Resolution on Privacy Protection in Social Network Services of October 2008; and the position paper published by the European Network and Information Security Agency (ENISA) on Security Issues and Recommendations for Online Social Networks of October 2007. For references, see footnotes 2 – 4 in the Opinion.
[18] Article 29 Working Party Opinion on online social networking (Opinion 5/2009 of 12 June 2009), section 3.1.1, *Purpose and nature*, on p. 6.
[19] "*Internet of the future: Europe must be a key player*" speech from Ms Reding, European Commissioner for Information Society and Media during the meeting Future of the Internet initiative of the Lisbon Council, Brussels, 2 February 2009. [original footnote]
[20] Article 29 Working Party Opinion on online social networking (Opinion 5/2009 of 12 June 2009), section 3.1.2, *Access to profile information*, on p. 6.
[21] Article 29 Working Party Opinion on online social networking (Opinion 5/2009 of 12 June 2009), section 3.1.2, *Access to profile information*, footnote 10, on p. 6.
[22] Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping (Reference for a preliminary ruling from the Göta Hovrätt), Opinion of Advocate-General Tizzano of 19 September 2002; Judgment of 6 November 2003, paras. 46 - 48. For a more extensive summary of that case (and other European case-law), see D Korff, *Paper No.4: The Legal Framework* (footnote 9, above), p. 42ff.
[23] Article 29 Working Party Opinion on online social networking (Opinion 5/2009 of 12 June 2009), section 3.1.2, *Access to profile information*, on p. 6.
[24] *Facebook et vie privée, face à face*, 16 January 2008, which can be found on: http://www.cnil.fr/index.php?id=2383
[25] *Blogs : la loi informatique et libertés s'applique mais ils sont dispensés de déclaration à la CNIL*, 31 January 2006 (with reference to its full Recommendation on the issue, contained in Deliberation No. 2005-285 of 22 November 2005). The advice (and a link to the full Recommendation) can be found on: http://www.cnil.fr/index.php?id=1939&news[uid]=305&cHash=5c85731663.
[26] *Facebook et vie privée, face à face* (footnote 22, above). Author's translation; reference to further restrictions on the dissemination of photographs of minors omitted.
[27] See: http://www.ico.gov.uk/Youth/section2/intro.aspx. There is no information aimed at others (like adults) on the ICO website, and in particular no suggestion that anyone uploading information on to the "Web" might come to be regarded as a controller, subject to the full force of the law.
[28] For an analysis of that case-law, see Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights, 1995, Chapter 11; Monica Macovei, Freedom of Expression: a guide to the implementation of Article 10 of the European Convention on Human Rights, Council of Europe Human Rights Handbook No. 2, 2001.
[29] Article 29 Working Party Recommendation 1/1997 on Data protection law and the media (WP1 of 25 February 1997).
[30] The right also includes the right to "seek" information, on the same basis, as is explicitly stipulated in Article 19 of the International Covenant on Civil and Political Rights. The omission of this word from the ECHR is generally accepted not to indicate any restriction on that right; the right to freedom of expression in the ECHR and the ICCPR are broadly applied in the same way.
[31] See Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights (footnote 26, above), pp. 12 - 15; Monica Macovei, Freedom of Expression: a guide to the implementation of Article 10 of the European Convention on Human Rights,
[32] The phrases are taken from paras. 84 – 90 of the ECJ's Lingvist judgment (footnote 22, above).
[33] D Korff, Comparative Summary of National Laws (footnote 1, above), section 10.1. The text prosented here has been somewhat redacted and in places updated.

[34] 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, published by the Swedish Helsinki Committee for Human Rights, Stockholm, 2001.

[35] 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 one 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.

[36] 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.

[37] 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, 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).

[38] QBD, Morland J., 27 March 2002.

[39] See D Korff, *Der EG-Richtlinienentwurf über Datenschutz und "anwendbares Recht"*, in: Recht der Datenverarbeitung, Year 10 (1994), Vol. No. 5- 6, p. 209 ff.

[40] Directive 95/46/EC has become part of the *acquis* of the European Economic Area (EEA). The question of whether the three non-EU EEA States (Iceland, Liechstenstein and Norway) should, for the purposes of the Directive, and more particularly for the purpose of Article 4, be treated as EU Member States or as "third countries" was initially not clear. Apparently, the Legal Service of the Commission has resolved that they should be treated as EU Member States for these purposes. Some national laws do not yet clearly reflect this, but this can presumably usually be resolved through interpretation. For the purpose of this paper, the words "EU Member States" therefore also cover the non-EU EEA States.

[41] Cf. Hondius, "*A Decade of International Data Protection*," in: Netherlands International Law Review**,** Vol. XXX (1983, p. 103ff, at 119ff. See also, by the same author, the paper "*Grenzüberschreitender Datenverkehr aus der Perspektive eines zukünftigen europäischen Datenschutzrechts***"** (*Referat für die 5. Datenschutzfachtagung*), Cologne, 1981, pp. 6–7.

[42] For an overview of no less than nine different possible solutions, see Michael Bergmann, "grenzüberschreitender Datenschutz," Baden-Baden, 1985, in particular Chapter 7: "*kollissionsrechtlicher Lösungsansatz*."

[43] COM(92)422 final–SYN 287, 15 October 1992, p. 13.

[44] *Idem*.

[45] D Korff, Data Protection Law in Practice in the European Union (footnote 1, above), Chapter 2, section iv; D Korff, *Der EG-Richtlinienentwurf über Datenschutz und "anwendbares Recht"* (footnote 7, above).

[46] This is expressly confirmed in the Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites **(**WP56 of 30 May 2002), section 2, on p. 6 (second paragraph).

[47] Strictly speaking, the Directive allows for data which are collected for certain "specified, explicit and legitimate purposes" to be further processed "*in a* ***way*** *[that is not] incompatible with those purposes.*" (Art. 6(1)(b)). But in practice this is read as allowing for processing of personal data for secondary purposes that are deemed to be "not incompatible" with the primary purpose for which the data were obtained.

[48] On this point, the UK Data Protection Act is clearly in violation of the Directive, in that it includes "medical research" in the wider list taken from Article 8(3) of the Directive, and thus uncritically allows secondary use of patient data for such reasearch, without bothering about the consent of the patients. See Schedule 3, Paragraph 8(2), to the Act. This is also directly contrary to the view of the Article 29 Working Party in its Working Document on the processing of personal data relating to health in electronic health records (EHR) (WP131 of on 15 Febnruary 2007). This is just one example of a provision which, if applied to data on patients in other EU Member States (as can easily happen under the rules discussed in this section), could cause serious conflicts with basic principles of data protection law in those other States.

[49] See the Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002), section 2.1, on p. 8, with reference to Case C-221/89 Factortame [1991] ECR I-3905 §20.
[50] Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002), section 2, on p. 6 (fifth paragraph).
[51] Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002), section 2, p. 7. Note that the document goes on to say that "*It is the location of the processing equipment used that counts*," but that comment only applies to non-EU-based controllers. For EU-based controllers, the determining factor is the country of establishment of the controller. If the controller is established in an EU Member State, and processes data on non-EU citizens, anywhere in the world, "in the context of the activities" of that establishment in that EU Member State, it must apply its national data protection law extra-territorially to the processing of the data on those non-EU (and non-EU-based) individuals.
[52] Article 29 Working Party Opinion on data protection issues related to search engines (WP148 of 4 April 2008), p. 9.
[53] Note that most of the other language versions of the Directive use a term that translates into English as "means" rather than "equipment" (F: *moyens*; I: *mezzi*; P: *meios*; Sp: *medios*). This terms suggests an even wider concept, not limited to any physical apparatus.
[54] The Danish law uses the term "*hjælpemidler*", which is somewhere between "means" and "equipment" (cf. the German *Hilfemittel*), while the Swedish law uses "*utrustning*", which is closer to "equipment" (cf. the German *Ausrüstung*).
[55] See footnote 6, above. For an early discussion (prior to the 2002 WP29 Working Document, WP56), see D Korff, European data protection law & the Internet, also mentioned in that footnote.
[56] See footnotes 17 – 21, above.
[57] Article 29 Working Party Opinion on data protection issues related to search engines (WP148 of 4 April 2008).
[58] Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002), section 1, in particular pp. 3-4.
[59] The so-called "PNR" controversy. On this, see D Korff, *Paper No. 3: The Use of New Technologies for Policing Purposes: the cases of the US TIA System & of the PNR Controversies*, in: I Brown & D Korff, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2004. See also the Article 29 Working Party Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities (WP151 of 15 February 2007, as revised and adopted on 24 June 2008) and its earlier Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America (WP97 of 30 September 2004).
[60] See the recent Article 29 Working Party Working Document 1/2009 on pre-trial discovery for cross border civil litigation (WP158 of 11 February 2009). Note in particular the following comment: "It is important to note that the US judge considers that if the company is subject to US law and possesses, controls, or has custody or even has authorized access to the information from the US territory (via a computer) wherever the data is 'physically' located, US law applies without the need to respect any international convention such as the Hague Convention." (footnote 4, on p. 5).
[61] Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002), section 2, p. 7.
[62] This is not the case if the equipment is only used for the purpose of transit through the territory of the Community. [original footnote]
[63] Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002), section 2.1, p. 8.
[64] Directive 2000/31/EC, Recital 19. [original footnote]
[65] Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002), section 2.4, pp. 9 – 10.

[66] Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002), section 3, Case A, p. 11.
[67] Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002), section 3, Case B, p 12..
[68] See the cover-page story of Time magazine by COHEN, Adam on 31 July 2000: *How to protect your privacy: who's watching you? They're called E.T. programs. They spy on you and report back by "phoning home". Millions of people are unwittingly downloading them.* [original footnote]
[69] See footnote 27, above.
[70] The more detailed information can again be found, as far as the Directive is concerned, in D Korff, Data Protection Law in Practice in the European Union, and as far as the national laws are concerned, in D Korff, Comparative Summary of National Laws, and in the *Country Reports* prepared in connection with data Protection Law in Practice in the EU (see footnote 1, above for all of these). Some further detailed information is also contained in the "*Commentary*", prepared in the context of the EC "e-TEN" project "EuroPriSe": see https://www.european-privacy-seal.eu/.
[71] Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP136 of 20 June 2007).
[72] *Idem*, p. 3.
[73] For the full discussion, of data on deceased persons, the unborn, and legal persons, see WP136 (footnote 71, above), section III.4, "*Fourth Element: 'Natural Person'*", pp. 21 – 24.
[74] WP136 (footnote 71, above), p. 24.
[75] In the UK, the courts have failed to apply the law in this way, and limited data protection unduly to "purely private" matters: see sub-section (b), below.
[76] See: Kovesi P., Video Surveillance: Legally Blind?, Proc. Aust. Pattern Recognition Society conference (DICTA09) pp. 204-211, IEEE Computer Society, December 2009, at http://www.csse.uwa.edu.au/~pk/Research/pkpapers/legallyblind.pdf.
[77] WP136 (footnote 71, above), pp. 8 – 9.
[78] See Council of Europe Recommendation No. Rec (2006) 4 of the Committee of Ministers to Member States on research on biological materials of human origin, of 15.3.2006. [original footnote]. See also the Article 29 Working Party documents on biometrics (WP80) and on genetic data (WP91) [added by DK].
[79] WP136 (footnote 71, above), p. 10.
[80] WP136 (footnote 71, above), p. 10.
[81] WP136 (footnote 71, above), p. 17 (in Example No. 15).
[82] WP136 (footnote 71, above), p. 17 (in Example No. 15). Note that in the Opinion, this example is given in a different context, concerning identifiability. However, it is clear from the quoted text that this is also an example of the application of the "purpose" criterion, applied in the context of the question of whether data "relate" to an individual. In the Opinion, a somewhat less illustrative example is given, relating to the keeping of telephone call records from a company's telephones.
[83] WP136 (footnote 71, above), Example No. 8, on p. 11.
[84] See WP136 (footnote 71, above), section III.3, "*Third Element: 'Identified or Identifiable' [Natural Person]*", pp. 12 – 21.
[85] Note that the system as here described is fundamentally different from the situation in which a trusted customer is provided with a hand-held scanner, and herself scans in the items she places in the trolley: in that situation, the customer is fully identified to the shop, and all the purchases are directly linked to the customer record.
[86] WP136 (footnote 71, above), p. 13, emphasis added.
[87] *Idem*, emphasis again added.
[88] *Idem*.
[89] *Idem*, Examples Nos. 14 and 15, on pp. 16 – 17. See also Example No. 16, about the retention of the "signatures" of graffitti artists etc.
[90] *Idem*, p. 18. On the technical aspects, the Opinion adds that "*Pseudonyms should be random and unpredictable. The number of pseudonyms possible should be so large that the same pseudonym is never randomly selected twice. If a high level of security is required, the set of potential pseudonyms must be at least equal to the range of values of secure cryptographic hash functions.*" (p. 18) In this, the Working Party refers to the October 1997 Working document "Privacy-enhancing technologies" by the Working Group on "privacy enhancing technologies" of the Committee on "Technical and organisational aspects of data protection" of the German Federal and State Data Protection Commissioners, published on

http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm (*idem*, footnote 13). This may be somewhat outdated by now.

[91] *Idem*, p. 19, in Example No. 17.

[92] *Idem*, pp. 19 – 20.

[93] *Idem*, p. 20.

[94] Email tothe author, July 2009. A more sophisticated, but still eminently readable discussion of this issue (and related issues) can be found in Ross Anderson, Security Engineering: A guide to building dependable distributed systems, 2001, Chapter 8, available free from: http://www.cl.cam.ac.uk/~rja14/Papers/SE-08.pdf. A new edition has been released in 2005: http://www.cl.cam.ac.uk/~rja14/book.html.

[95] See also: Ian Brown, The Limits of Anonymisation, on the Privacy Value Networks website: http://www.pvnets.org/2009/03/the-limits-of-anonymisation/, with reference to the work of Arvind Narayanan and Dr Vitaly Shmatikov of the University of Texas at Austin on de-anonymisation of data from SNS websites, availabe from: http://33bits.org/2009/03/19/de-anonymizing-social-networks/. See also the recent and (for non-computer experts) seminal paper by Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, Colorado Law, Legal Studies Research Paper Series, Working Paper Number 09-12, August 13, 2009, available online from: http://ssrn.com/abstract=1450006.

[96] See, e.g., P Serge Gutwirth and Mireille Hildebrandt, Profiling the European Citizen, International Conference Computers, Privacy & Data Protection, 16 & 17 January 2009, Brussels Belgium, Text of the presentation by Serge Gutwirth on 17 January 2009: http://www.cpdpconferences.org/presentations.html.

[97] As the ACLU put it, with reference to two earlier reports into surveillance in the USA (Bigger Monster, Weaker Chains, 2003, and The Surveillance-Industrial Complex, 2004): "*One of the most alarming trends that we identified in our earlier reports was the turn by our security establishment toward suspicionless mass surveillance as a central strategy in the so-called 'war on terror'.*" The most advanced project of this kind was the so-called "Total Information Awareness" system developed in the (mis-named) US "War On Terror"; on this, see Douwe Korff, *Paper No. 3: The Use of New Technologies for Policing Purposes: the cases of the US TIA System & of the PNR Controversies*, in: I Brown & D Korff, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2004. The same is however happening in European countries: cf. the discussion of the parliamentary debate on the UK Serious Crime Bill 2006-07, in Douwe Korff, Guaranteeing Liberty or Big Brother: Surveillance in the United Kingdom, presentation at the 2007 Summer Academy of the Schleswig Holstein Independent Privacy Protection Centre (ULD), Kiel, 24 August 2007, pp. 16 – 17. The presentation can be found at: https://www.datenschutzzentrum.de/sommerakademie/2007/. "Profiling" and "data mining" are also increasingly encouraged - indeed required - at the European level.

[98] Cf., for instance, the finding that with certain facial recognition software "*groups classified as 'Asians' and 'African Americans' were easier to recognise than Caucasians because the facial recognition software was programmed to search for the supposedly distinct physical characteristics of such populations*." - A Report on the Surveillance Society, produced for the Information Commissioner by the Surveillance Studies Network, September 2006, Expert report on "*Infrastructure and Built Environment*", p. 7. The full report, as well as the appendices (including a number of expert studies) and a summary report can all be downloaded from the ICO website: http://www.ico.gov.uk/ (type "surveillance society" into the search box: it is difficult to find through other links). The Surveillance Project's own website is: http://www.queensu.ca/sociology/Surveillance/. See also more generally the discussion on pp. 6 – 7 of the expert report.

[99] See generally, the section on "*Risks & Limitations*", in: Douwe Korff, Guaranteeing Liberty (note 97, above), p. 52ff.

[100] The latter phrase is used by the UK Information Commissioner in his criticism of proposals for "data mining" in the UK. On the general issue, see the extremely useful blog entry "*Data Mining for Terrorists*" on the website *Schneier on Security*, http://www.schneier.com/blog/archives/2006/03/, quoted in full (with further references, including a link to a CIA book confirming this limitation) in Douwe Korff, Guaranteeing Liberty (note 97, above), under the heading "*data mining*", pp. 63 – 66.

[101] This is a particularly serious issue in the UK: see Douwe Korff, Guaranteeing Liberty (note 93, above), *passim*.

[102] Gutwirth and Hildebrandt (footnote 96, above) seem to rely only on the "content" criterion in this regard, and thus seem to believe that "profiles" (and location and traffic data) usually do not constitute "personal data", but they effectively apply the "purpose" and "result" (effect) criteria when they argue that all these data should be brought within the law: "That is why we think that '*profiling' calls for a system of protection of individuals against the processing of data that impact upon their behavior even if those data cannot be considered as personal data*, which implies a shift from the protection of *personal* data to the protection of data *tout court*! … It might seem so, but in fact this is not a revolutionary step since it just picks up the tread opened by the

Directive 2002/58 which, in order to protect privacy, provided for the protection of location and traffic data (which are not necessarily 'personal data')." (at p. 4, original italics).

[103] Draft Recommendation On The Protection Of Individuals With Regard To Automatic Processing Of Personal Data In The Framework Of Profiling.

[104] Again, leaving aside the fact that some extend their law, sometimes through an extension of the definition of "data subject", to "legal persons"; and that some extend some protection to the deceased and unborn, where others don't: cf. foonote 73, above.

[105] *Panta rhei*, "everything is in a state of flux" (the word *rhei* is simply the Greek word for "to stream"). According to the Wikipedia entry on the philosopher, the words were either not actually spoken by him (or if they did, do not survive as a quotation from him), but are an aphorism used by Simplicius to characterise Heraclitos' thinking. See: http://en.wikipedia.org/wiki/Heraclitus.

[106] Note the policy of the search engine "*Ixquick*", which (since January 2009) no longer records any IP addresses of its users at all. It is the first and, to date, only search engine to do this, and was awarded the first European Privacy Seal for its data protection friendly policy: http://www.ixquick.com/uk/protect_privacy.html.

[107] Constitutional Court Judgment (*BverfGE*) of 04.04.2006 (File Ref. 1 BvR 518/02).

[108] Summary from the webpage of the Bavarian data protection authority: http://www.datenschutz-bayern.de/tbs/tb22/k4.html#4.8, at 4.8, *Rasterfahndung*. (translated by the author).

[109] *Idem.*

[110] *Idem.*

[111] Private-sector databases are undoubtedly increasingly "trawled" through and used to "profile" people for public-sector/law enforcement/anti-fraud/anti-terrorist purposes: cf. the SWIFT and PNR controversies (footnote 59, above). We are not aware of the use of police or anti-terrorist databases in the private sector (although there may be in relation to the hiring of people for "sensitive" jobs), but other public-sector records and databases, from population registers to company directors' registers, are widely used for private sector activities, including marketing and credit scoring.

[112] Cf. the text of the definition in the Directive, quoted at (a).

[113] On that issue, see the quite detailed discussion in Douwe Korff, Comparative Summary (footnote 1, above), section 2.4, at p. 26ff.

[114] Strictly speaking, the Framework Directive refers to processing ***in a way*** that is [not] incompatible with the specified purpose, rather than to processing for a secondary purpose that is incompatible with the primary purpose. In practice, both the Article 29 Working Party and the national DPAs tend to focus on the compatability of the primary and secondary purposes.

[115] See Douwe Korff, The feasibility of a seamless system of data protection rules for the European Union , Study for the European Commission (1996 – 97, published 1999).

[116] See the WP29 "Working Document on the processing of personal data relating to health in electronic health records (EHR)", WP131 of 15 February 2007. Note: The implications of ill-defined purposes in legal rules, and of seeking "consent" for processing for insufficiently-defined purposes, are discussed at iv. The multiple ramifications of the need to narrowly define purposes in itself underlines the importance of further guidance and harmonisation in this regard.

[117] Processing of "sensitive data" must conform to the data protection principles and to the stricter rules of Article 8, discussed in section 4.4, below.

[118] For further detail, see Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe Korff, Privacy & Law Enforcement, study for the Information Commissioner, 2004, pp. 8 – 15, from ICO website: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/legal_framework.pdf; Douwe Korff, The need to apply UK data protection law in accordance with European law, Data Protection Law & Practice, May 2008.

[119] This phrase is used here to cover the two criteria contained in paras. (c) and (e) of Article 7 of the Directive, i.e.: "processing [that] is necessary for compliance with a legal obligation to which the controller is subject" and "processing [that] 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". Specifically, we may note that the "legal obligations" referred to in Article 7(c) are not those derived from a contract or pre-contractual situation, since these are covered by Article 7(b); and that the "tasks" and "authority" referred to in Article 7(e) will be tasks and powers granted by law.

[120] See footnote 118, above.

[121] See, e.g., Copland v. the UK, ECtHR judgment of 3 April 2007; S. & Marper v. the UK, ECtHR GC judgment of 4 December 2008. Further ECtHR cases relating to personal data are discussed in Douwe Korff, *The Legal Framework*, o.c. (footnote 118, above).

[122] The German Telecommunications Data Protection Law, even in its previous form, did (and in its current, revised form still does) prohibit the requiring of consent for secondary processing as a condition for the provision of a service.

[123] See the WP29 "Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools)", Working Document 1/2008 (WP147) of 18 February 2009. See also Terri Dowty & Douwe Korff, Protecting the virtual child: the law and children's consent to sharing of personal data, Action for Children's Rights (ARCH)/Nuffield Foundation, January 2009. The latter report contains a comparative-legal overview of the law in EU MSs: see pp. 27ff.

[124] See the WP29 "Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP114 of 25 November 2005), p. 10-12.

[125] *Idem*, p. 11.

[126] See the WP29 document referred to in the previous footnote.

[127] WP29 "Working Document on the processing of personal data relating to health in electronic health records (EHR)" (WP131 of 15 February 2007, p. 9)

[128] See the Article 29 Working Party Working Document on biometrics (WP80 of 1 August 2003), its Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS) (WP96 of 11 August 2004) and Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (WP112 of 30 September 2005). It included a definition of biometric data in its Opinion on the concept of personal data (WP136) (with reference to a Council of Europe Recommendation).

[129] See the Article 29 Working Party Opinion 6/2000 on the Human Genome and Privacy (WP34 of 13 July 2000) and its Working Document on Genetic Data (WP91 of 17 march 2004).

[130] Authorisation No. 1/2008 Concerning Processing of Sensitive Data in the Employment Context, 19 june 2008, available in English from: http://www.garanteprivacy.it/garante/doc.jsp?ID=1640699

[131] Executive Summary of the final draft of the Comparative Legal Study on assessment of data protection measures and relevant institutions, report commissioned by the Fundamental Rights Agency (FRA) of the European Union (2009), para. 8.

[132] These are, respectively: Opinion 8/2001 on the processing of personal data in the employment context (WP48 of 13 September 2001); Recommendation 1/2001 on Employee Evaluation Data (WP42 of 22 March 2001); Working document on the surveillance of electronic communications in the workplace (WP55 of 29 May 2002); and Opinion 2/2006 on privacy issues related to the provision of email screening services (WP118 of 21 February 2006).

[133] Note that the rights discussed in this section are backed up by procedural rights: the right to a judicial remedy against any breach of the substantive rights (Art. 22); the right to an administrative remedy against processing which violates an individual's right to data protection (in particular in the form of an appeal to the national data protection authority) (Art. 28(4)); and the right to obtain compensation for damages resulting from processing in contravention of the national laws implementing the Directive (Art. 23). These latter rights relating to individual remedies are discussed separately in Part 5, section 5.1. Other instruments (including the Council of Europe Convention on data protection) also contain a broader right of data subjects, to establish the existence of data files, and to be given details of such files. The Directive ensures the same, by requiring that the Member States establish a publicly accessible register of processing operations, and by stipulating that for non-notified operations, the same information must be made available to anyone, on request (Art. 21).

[134] Note that we will discuss the right to be informed of the "logic" used in the taking of fully automated decisions later, in the sub-section dealing with those kinds of decisions, rather than here, in the more general sub-section of the right of access.

[135] Cf. the 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." This is the traditional distinction. Recent developments, including in particular the establishment of large-scale "data mines" (discussed in Working paper No. 1), 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.

[136] Separate Fax- and Telephone Preference Services have also been established in several countries, and a (not quite as effective) e-MPS has been created for the Internet, but these relate to the more specific rights under the e-Privacy Directive and will therefore not be discussed here. For details, see the Guide to Robinson Lists and

Preference Services, published by FEDMA (the Federation of European Direct Marketing): http://fedma.custompublish.com/index.php?cat=72109.

[137] See the 15th Annual Report of the CNIL and the brief reference to this case in the press release on that report, at: http://annuaire.in2p3.fr/legal/cnil-presse-rapport15.html.

[138] Dammann\Simitis, EG-Datenschutzrichtlinie: Kommentar, Baden-Baden, 1997, margin note 4 to Article 15.

[139] Article 4(2) of Directive 2002/58/EC stipulates that:

"In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved."

[140] Datenschutzfreundliche Technologien (Data protection-friendly technologies) (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.

[141] Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka, Modernisierung des Datenschutzrechts, Expert opinion commissioned by the Federal Ministery of the Interior, 2001, available from: http://www.computerundrecht.de/media/gutachten.pdf .

[142] *Säkerhet för personuppgifter*, latest (2008) version available from the DPA website, at: http://www.datainspektionen.se/Documents/faktabroschyr-allmannarad-sakerhet.pdf

[143] For a detailed discussion, see Chapter 7, in D Korff, Data Protection Law in Practice in the European Union (footnote 1, above). This covers in some detail the question of how "adequacy" is supposed to be determined, and the "Safe Harbor" arrangements with the USA.

[144] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:EN:PDF.

[145] *The Stockholm Programme – An open and secure Europe serving and protecting the citizens*, Brussels, 2 December 2009, Council Document 17024/09. The programme contains the following inspiring passages:

"The Union must secure a comprehensive strategy to protect data within the EU and in its relations with other countries. In that context, it should promote the application of the principles set out in relevant EU instruments on data protection and the 1981 Council of Europe Convention on data protection as well as promoting accession to that convention. It must also foresee and regulate the circumstances in which interference by public authorities with the exercise of these rights is justified and also apply data protection principles in the private sphere.

"The Union must address the necessity for increased exchange of personal data whilst ensuring the utmost respect for the protection of privacy. The European Council is convinced that the technological developments not only present new challenges to the protection of personal data, but also offer new possibilities to better protect personal data.

"Basic principles such as purpose limitation, proportionality, legitimacy of processing, limits on storage time, security and confidentiality as well as respect for the rights of the individual, control by national independent supervisory authorities, and access to effective judicial redress need to be ensured and a comprehensive protection scheme must be established."

The programme does not yet explain how this is to be achieved - which is a major and central challenge.

[146] See the quote from the UK Information Commissioner on p. 180 of the Comparative Summary (footnote 1, above).

[147] WP29 "Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (footnote 12, above), p. 4.

[148] *Idem*, Executive Summary, p. 2.

[149] Comparative Legal Study on assessment of data protection measures and relevant institutions, commissioned by the Fundamental Rights Agency (FRA) of the European Union (EU) and carried out under the leadership of Professor Martin Scheinin at the European University Institute, 2009. The author of the current paper prepared the country report on the UK for this study, on behalf of the Human Rights Centre of the University of Nottingham. The general report and the country reports are due to be published in the autumn of 2009.

[150] See Harris, O'Boyle & Warbrick, o.c. (footnote 27, above), Chapter 14.

[151] Article 29 Working Party, Working Document on Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive (WP12 of 24 July 1998), p. 13.

[152] The *Qui tam* principle allows individuals (possibly backed by organisations/NGOs) to pursue alleged violations of the law (in our case, that would be of data protection law), with the offer of being awarded not just full costs but also a reward if the action is succesful. It is enshrined in a US federal law, under which it can apparently be widely used.

[153] Note that the Member States may designate separate authorities for separate areas - including special authorities to supervise processing most likely to benefit from derogations under Article 13, such as processing by the police or the security services.

[154] Douwe Korff, Existing case-law on compliance with data protection laws and principles in the Member States of the European Union, Study for the European Commission, 1997, published 1998; Comparative Legal

Study on assessment of data protection measures and relevant institutions, footnote 112, above. Although the first of these studies is by now quite old, regrettably, the deficiencies in data protection enforcement noted in it will be shown to have remained in the second, broader and very recent study.

[155] Douwe Korff, *Country Report on the UK*, 2009, for the Comparative Legal Study on assessment of data protection measures and relevant institutions, footnote 112, above.

[156] *Idem*.

[157] The Directive as such merely stipulates that the DPAs "shall act" in this manner, but this presupposes that the Member States make it functionally and otherwise possible for them to do so.

[158] See Dammann/Simitis, EGDatenschutzrichtlinie - Kommentar, Baden-Baden, 1997, Commentary on Article 28, point 4, margin note 10, on p. 310.

[159] For fuller detail, see the Comparative Legal Study on assessment of data protection measures and relevant institutions, footnote 112, above.

[160] See Douwe Korff, Comparative Summary (footnote 1, above), pp. 162 – 164 for detail.

- o –O – o -