Recommendations from PRIVIREAL to the European Commission

Introduction

The purpose of PRIVIREAL was first to evaluate the implementation of the Data Protection Directive in Member States Law, second to assess the way that Research Ethics Committees operate in relation to data protection law, and third, on the basis of the first two evaluations, to make such recommendations as the membership felt necessary both to the Commission and to their individual Member States to ensure the better protection of data subjects in medical research in line with the purposes of Directive 95/46/EC.

The recommendations that follow present the case for particular responses to difficulties identified by PRIVIREAL in three ways: first, where there is a strong consensus amongst PRIVIREAL's membership and where the membership feels that a course of action is necessary, there that course of action is argued in detail and is clearly stated; second, where the argument indicates that a course of action, while not necessary, could be followed, the recommendation is made without the force of the first position; third, where it is clear to the membership that guidance is required, but equally there was no consensus between the membership of what the guidance should be, the arguments for each side of the arguments are presented and the need for a political decision is stated. All the recommendations are made, in this chapter, to the Commission. Recommendations to individual Member States are made elsewhere in this volume.

The recommendations focus around the following: (a) Article 8; (b) Articles 10 and 11; (c) anonymisation and the definition of personal data; (d) the research exemption; (e) explicit consent; (f) data relating to dead people; (g) prior checking; (h) Article 13; (i) third country data transfers; (j) RECs and data protection in medical research; (k) data protection and genetic information; (l) the question of the need for a specific Directive on data protection in medical research.

(a) Recommendations around Article 8

According to Article 8.1 the processing of special categories of personal data is prohibited. However, Article 8.2–5, in circumstances specified, permits Member States to lift this prohibition. A list of alternative conditions of legitimate processing is presented in Article 8.2, and this includes the explicit consent of the data subject. Article 8.3 states that the prohibition does not

apply for processing for medical purposes by a health professional or someone under an equivalent duty of professional secrecy, and, according to Article 8.4, Member States may extend the conditions of legitimate processing by national law or decision of the supervisory authority in the substantial public interest.

The relationship between Article 7 and 8 is also of some interest. Is it plausible to consider satisfaction of Article 7 to be a sufficient condition for the lawful processing of personal data that is not within the special categories, and satisfaction of Article 8 to be a sufficient condition for the lawful processing of special categories of personal data? We think not. First, Article 7 provides positive conditions to legitimate processing whereas Article 8 merely removes a prohibition, which suggests that special categories of personal data are to be considered a subcategory of personal data that is subject to Article 7. Secondly, the Directive lays down additional conditions for lawful processing, because Articles 6, 7, 10, and 11, amongst others, lay down additional conditions for legitimate processing. Nevertheless experience reveals that this is not always clear to data controllers. For example, while the UK has implemented Articles 7 and 8 in Schedule 2 and 3 of the Data Protection Act 1998 clearly indicating that lawful processing of special categories of personal data require satisfaction of a condition derived from each Article as a necessary but not necessarily sufficient condition, the UK has also passed regulations under Section 60 of the Health and Social Care Act 2002 that render certain processing (including for medical research) of personal health data without the patient's consent not a breach of the common law on confidentiality. The conditions that must be satisfied are, in our opinion, sufficient to satisfy not having to obtain explicit consent in the terms of the Data Protection Directive (on which see further below). However, they are not in our opinion sufficient to render the processing lawful in the terms of the Data Protection Directive because they do not require patients to be informed when data is taken from them that their data may be used for research. The wording of the Health and Social Care Act in relation to this is, however, ambiguous, as it is stated that when the conditions of regulations under the Act are satisfied then processing is to be taken to be lawfully done despite being in breach of confidentiality. This is likely to be read as meaning that nothing more needs to be done to render the processing lawful, when all it can mean is that the processing is not to be taken to be unlawful (and thus a breach of the Data Protection Act 1998/Directive via a breach of the principle that processing must be lawful; and fair) on account of being a breach of confidentiality. Consequently, we recommend that

- **The Commission should specify in guidance that while processing of special categories of personal data will be unlawful unless a**

condition of legitimate processing under Article 8 is satisfied, satisfaction of such a condition will not by itself necessarily render processing lawful.

In relation to Article 8.3, the question arises as to whether or not medical research may be considered to be a purpose covered by Article 8.3 (as, e.g., the UK and the Irish law maintain). Alternatively, it is possible to legitimate medical research pursuant to Article 8.4 by specifying it to be in the substantial public interest. However, it is arguable that not all medical research is in the substantial public interest, and, if so, Article 8.4 may only be used for categories of medical research that are in the substantial public interest.[1] Difficulties here arise because the Directive does not explicitly define what categories of processing for investigative processes constitute research. Without such a definition, it becomes arguable, though contestable, that because medical research is for purposes of prevention of disease or might assist with medical diagnosis (processes that are included under Article 8.3), that research is covered by Article 8.3. It is arguable that this falls under the discretion of individual Member States. However, variation in the definition of medical research will clearly affect uniform implementation of the Directive in relation to the protection of fundamental rights and freedoms.

In relation to these issues we recommend that
The Commission should issue guidance on

- **Whether or not medical research may be considered to be a purpose under Article 8.3**
- **The definition of "medical research"**
- **Whether all medical research may be considered to be in the substantial public interest under Article 8.4**
- **The general characteristics of what might be considered to be in the substantial public interest as against in the public interest but not substantially so, should its opinion be that all medical research is not necessarily in the substantial public interest**

The options under Article 8.2 are not explicitly accorded any relative importance or priority in relation to each other. However, Article 1.1 of the Directive specifies that the objective of the Directive is to protect fundamental rights and freedoms, in particular, privacy, in the processing of personal data.

[1] In relation to this, the UK, in passing a statutory instrument to legitimate research in the substantial public interest has implicitly recognised that not all research is in the substantial public interest, but leaves open the question as to whether all medical research might be held to be in the substantial public interest.

Fundamental rights and freedoms include those protected under the ECHR and the European Court of Human Rights has held (see, e.g., *M.S. v Sweden*[2]) that to use personal medical information without explicit consent engages the right to private life under Article 8.1 ECHR, with the implication that to process personal medical information without explicit consent is a violation of Article 8.1 ECHR unless justified in the terms of Article 8.2 ECHR. From this, it seems to follow that legitimating conditions other than explicit consent of the data subject may only be appealed to if explicit consent is impracticable, inappropriate, or disproportionate in relation to conflicting legitimate needs etc.[3]

Given that the legislation in Member States often does not specify that prima facie priority is to be given to explicit consent under Article 8.2 of the Directive[4], we recommend that

- **The Commission address the question of the explicit consent under Article 8.2 of the Directive in relation to the requirements of Article 8 ECHR and should indicate in guidance that explicit consent must take priority over other conditions unless appropriate derogation per Article 8.2 ECHR applies**

Connected with this, we recommend, since the position is less clear[5], that

---

[2] (1997) 28 EHRR 313, paragraph 34. See also *Z v Finland* [1997] ECHR 10 (25 February 1997), paragraphs 96-97 and also *Peck v United Kingdom* [2003] ECHR 44 (28 January 2003), paragraphs 78-80 (although the latter did not concern medical data)

[3] While consent respects the right to privacy in particular, none of this is to suggest that there are no difficulties in securing reliable and adequate consent, nor is it to suggest that once consent has been obtained no efforts need to be made to safeguard the processing of personal data in other ways required by the Directive.

It is arguable that, in the specific cases of epidemiological research or public health research, processing without consent would satisfy the conditions of Article 8.2 ECHR.

[4] For example, the view of the Supervisory Authorities in Germany and in the UK is that explicit consent is not to be given a specific priority. On the other hand, in Portuguese Constitutional law, consent is required generally in such cases, which affects Portugal's implementation of the Directive. (This, however, does not enable us to infer that Portugal itself interprets the Directive as requiring explicit consent.) Equally, priority is given to consent in practice in Norway.

[5] Because there is no relevant jurisprudence from Strasbourg on simple non-explicit consent and the Directive itself is not fully clear about the difference between explicit consent and mere consent.

- **The Article 29 Working Party address the question of whether or not priority is to be given in Article 7 to consent for processing and also the question of whether non-explicit consent coupled with an Article 8 (of the Directive) condition for lifting the prohibition on processing of special categories of data can substitute for explicit consent without satisfying the conditions of Article 8.2 ECHR for not obtaining explicit consent when special categories of data are being processed**

(b) Recommendations around Articles 10 and 11

Article 10 requires Member States to impose a duty on data controllers to supply the data subject with specific information about intended processing of personal data where data was obtained from the data subject. Article 11.1 requires Member States to impose a duty on data controllers who did not obtain personal data from the data subject to provide the data subject with similar information. Article 11.1 may be derogated from on the grounds of impossibility, disproportionate effort, or legal provision; but no similar derogation from Article 10 is provided, though Article 13.1 does permit Member States to modify Article 10 (amongst others) for a number of purposes, including in the interests of the data subject or the rights and freedoms of others. Unless Member States have made available a path via Article 13 (about which see below), this suggests that where a data controller obtained personal data from a data subject and wishes to process the data for purposes not anticipated or envisaged at the time that the data was obtained from the data subject (so that the data subject was not informed of these purposes), the data controller must now contact the data subject and provide the data subject with the prescribed information before the data may be processed for the intended purpose. However, Recitals 39 and 40 seem to state, even for the case where information was obtained from the data subject, that the duty to provide information about unanticipated disclosures to third parties may be derogated from where this is impossible, would involve disproportionate effort, or where there is legal provision made. It is arguable, by purposive construction, that such a derogation may be extended to unanticipated processing generally where personal data was obtained from the data subject (because once the data is in the hands of a third party, the provision of information for purposes of processing determined by the third party are subject to such a derogation under Article 11.2). The permissibility of appeal to Recitals 39 and 40 in this way would considerably ease the burden on data controllers who later wish to process for purposes (including research) that they did not inform the data subject about because they did not envisage that they might wish to do so at the time the data was obtained. However, the import of Recitals in relation to Articles is a matter of some controversy, and even if Recitals 39 and 40 can be read to create a derogation

for unanticipated disclosures under conditions similar to those provided by Article 11.2, some might consider the extension to processing for unanticipated purposes to be teleological interpretation taken too far. Furthermore, even those who consider that this would be a perfectly proper use of teleological interpretation might consider that this construction does not go far enough to satisfy the deeper objectives of the Directive in relation to processing for research. In other words, they will contend that, given that data to be used for research may be kept indefinitely under certain circumstances, that the use of Recitals 39 and 40 to create a derogation from some Article 10 situations does not go far enough.

Divergent interpretations of Articles 10 and 11 by the Member States reflects uncertainty about the best interpretation of the Directive on these points. For example, Italy does not permit any derogation where data was collected from the data subject. Some others provide an exemption on the grounds of impossibility and disproportionate effort in the Article 10 situation as well as in the Article 11 situation, which in the general opinion of the group is not permissible. And although the UK and Ireland might be thought to fall into the latter group, their implementation is open to another interpretation. Where data was obtained from the data subject ("the Article 10 case") the UK Data Protection Act 1998 (and the Irish Act) provides that the prescribed information be provided insofar as practicable. The problem here is not so much that "practicable" might be interpreted in a weaker way than "possible", because there is no provision (apart possibly from the Recital 39 and 40 cases/recourse to Article 13) for derogation on the grounds of impossibility from the duty to provide the prescribed information in the Article 10 case. In our opinion (subject to proviso in relation to Article 13, about which see below), this provision is illegitimate unless "insofar as practicable" means "insofar as envisaged" or else applies only to the detail of the Article 10 information to be provided and not to whether or not the Article 10 information needs to be provided at all.

Given that the general (but by no means unananimous) opinion of the group was in favour of teleologically extended interpretation via Recitals 39 and 40, we recommend

- **The Commission should issue an opinion on the permissibility of derogation from Article 10 via appeal to Recital 39 in conjunction with Recital 40, and extension of this to unanticipated processing generally**

Articles 10 and 11.1 prescribe that information other than that relating to the identity of the controller (or his representative) and the purposes of

processing need only be provided insofar as this is necessary for processing to be fair. It is our opinion, however, for reasons of purposive construction[6], that "fairness" (to be interpreted in terms of proportionality when derogating from Article 8.1 ECHR on grounds provided by Article 8.2 ECHR) should be the operative criterion when considering the detail of the compulsory information to be provided as well whether or not additional information is to be provided. The issue here encompasses questions of the following kind: "How specific must the information be that is given to potential data subjects"; "Is the information sufficient if it informs the data subjects generally that their data will be used for research purposes, or should the type of research or specific diseases it concerns be indicated?" It was widely felt that because research can cover many things, that simply to specify that data can be used for research is not adequate. However, it was not possible to come to a consensus over how the word should be precisely specified.

We recommend, therefore, that

- **The Commission must address the question and issue suitable guidance as to the degree of information that needs to be provided about particular purposes (e.g., research). In particular, is it sufficient to inform that the purpose is, e.g., for research, or must the kind of research and what it might involve be specified, and if so, to what degree? Also, is fairness the decisive criterion in relation to the degree of the compulsory information as well as additional information prescribed by Articles 10 and 11.1?** [7]

An example of additional information to be provided given by the Directive in Article 10 is "whether replies to the questions are obligatory or voluntary". In our opinion it can be just as important to inform data subjects about whether or not processing is obligatory or voluntary (i.e., whether or not they have the right to object to the questions posed by the data controller to elicit information or whether the right has been removed by law). This is not just important in relation to any use of Article 14(a) exemptions. It is also important where, e.g., conditions other than consent (especially explicit consent) are appealed to in order to legitimate processing in the terms of Articles 7 and 8 and where there is no exemption from the duty to provide information. This is particularly important when dealing with processing (including processing for research) in vulnerable populations (which patients generally are), whose members might not understand that they have the right

[6] This is. an interpretation that is governed by the need for the Directive to give effect to its objectives.

[7] A purposive or teleological construction suggests that it ought to be.

to object or be willing to do so, even if they know they have the right, unless they are reassured about their ability to do so, and this is even more important in specially vulnerable subgroups of patients.

We recommend that

- **In cases where there is no exemption from the duty to provide information, the Commission issue guidance to the effect that the provision of such additional information should be regarded as compulsory when processing is for medical research.**

Because of the central importance of the provision of information if data subjects are to be able to exercise their rights, special safeguards are required whenever there is an exemption from the duty to provide information to the data subject. We recommend, in relation to this that the Commission issue guidance to the effect that

- **Whenever there is such an exemption for processing involving special categories of data (especially in specially vulnerable populations) the processing must be subjected to prior checking as required under Article 20 of the Directive.**

(c) Recommendations around Anonymisation and the Definition of Personal Data

According to Recital 26, processing of all personal data is subject to the data protection principles, but once personal data is rendered anonymous so that the identity of the data subject is no longer ascertainable directly or indirectly the data protection principles no longer apply.

Article 2(a) defines personal data as information relating to an identified or identifiable natural person (an identifiable person being one who can be directly identified from the information or indirectly identified by, e.g., an identification number or by one or more factors specific to the person's physical, physiological, mental, economic, cultural or social identity. According to Recital 26, indirect identification must be reasonably likely, but may be by the controller or any other person. (It is clear from this that anonymised data is data rendered non-personal).

However the Directive only applies to personal data

(1) Processed wholly or partly by automatic means;
(2) Processed by non-automatic means, when it forms part of a filing system or is intended to form part of a filing system (Article 3.1);

provided further that it is

> Neither processed in the course of an activity that falls outside the scope of Community law (Article 3.2); nor processed by a natural person for purely domestic purposes (Article 3.3).

Personal data forms part of a filing system when it is structured so that it is readily accessible according to specific criteria.

There is a variety of understandings of the term "anonymisation" in general usage. From a legal point of view, however, the only definition of anonymisation that is relevant is that which is contained in the Directive. That is to say, only if data is rendered anonymous in the manner defined by the Directive do the data protection principles not apply. However, experience of those members of the group who are on ethics committees or work in the scientific community indicates that researchers have a tendency to regard data as having been rendered anonymous with the effect of placing it outside of the scope of data protection law when it is still retained in a form that according to the Directive means that it is still personal data. In effect, instead of detailing the way in which data is being processed and the form in which it is being kept in relation to the demands of the Directive, researchers simply claim that data has been rendered anonymous when what has been done to it does not render it anonymous under the Directive. The source of the problem is that while researchers fully appreciate the definition of "anonymisation" within their own professional practice and ethical culture, they do not fully appreciate that what is significant is the legal definition of "anonymisation" given by the Directive. The consequence is that even if there is no intention to do so, the use of the label "anonymisation" operates as a metaphor or an ideological tool to relieve researchers, at least in their own minds, from the need to comply with the law's demands.

We recommend that

- **The Commission issue guidance to discourage the use of the term "anonymisation" in favour of detailed statements about the form in which data is to be kept with particular attention being placed upon identifiers that have been removed but that can still be linked to the data.**

In general, anonymisation raises several questions. Suppose A, who obtains personal data from C, wishes to process it for purposes Q (or intends to pass it on to B for processing), but only after rendering it completely non-personal. Do the principles of protection apply to this processing? While Recital 26

might seem to suggest that it does not because the data processed has been rendered anonymous, it also states that the principles apply to it before it has been rendered anonymous. Because processing includes anything done to personal data (which must include rendering it anonymous) and Article 10 of the Directive requires data subjects to be informed of the intended purposes of processing, this suggests, at the very least, that data subjects must be informed about any intended anonymisation and any consequences of anonymisation necessary for fair processing. Suppose, instead that A who obtained personal data from C, intends to keep it a personal data but will pass on information taken from it to B for processing by B who will not be able to identify the person to whom it relates. Is A to be held responsible for the processing of this information by B? Or is the processing by B outside the scope of the principles because the data is not held in personal form by B? If the data is held to be within the scope of the Directive, is B to be held to have duties to the data subject or are the responsibilities entirely those of A?

In our opinion, answers to questions like these depend crucially on what the reasoning behind Recital 26 is, and this depends centrally on the concept of privacy with which the Directive operates. In relation to this, there are two concepts that need to be considered. First, there is a "narrow" conception of privacy, according to which privacy is concerned merely to protect the identity of the data subject. But there is a contrary "broad" concept of privacy according to which privacy seeks to give data subjects control over personal information on them that can negatively affect their physical, psychological and moral integrity. Under the narrow conception, to render personal data anonymous is to remove any interest that the data subject has in the use of it. Under the broad conception, rendering it anonymous merely protects against certain abuses of that data. (It does not, e.g., prevent personal information obtained from devout Catholics being used to develop chemical contraceptive methods, which is arguably contrary to their moral integrity). Correlated with the narrow conception, the point of Recital 26 is to emphasise that the data subject has no interest that the Directive recognises in what is done with personal data once it is rendered anonymous. Correlated with the broad conception, the point of Recital 26 is merely to recognise that once data is rendered anonymous, it is not *possible* for the principles of protection to apply and for data subjects to exercise the rights, and data controllers the duties, the Directive grants or imposes (correlative to which, if the context is such that *it is possible* for these rights and duties to be exercised or discharged then the data must be considered to be personal data and not rendered anonymous).

In the EU, some academics and some jurisdictions favour the narrow rather than the broad concept of privacy. For example, in the UK in the *Source Informatics* case, the Court of Appeal of England and Wales, in making

comments about the Directive, clearly supports the narrow concept of privacy.[8] On the other hand, the general jurisprudence of the European Court of Human Rights in relation to Article 8 of the ECHR is based upon a very broad concept of privacy.[9] The members of the PRIVIREAL group, though almost universally favouring a broad concept of privacy, were not absolutely unanimous on this. Clearly, a central issue here is what weight is to be given to the jurisprudence of the European Court of Human Rights in the interpretation of the Directive, because the stronger the persuasive force of the European Court of Human Rights is the more difficult it is to support the narrow interpretation of the concept of privacy in the Directive. The specific impact of choosing between a narrow and a broad concept of privacy includes the following contrasts:

1. Under a narrow conception of privacy, Recital 26 of the Directive indicates that data subjects lose all interest in processing of their data once it is rendered anonymous: under a broad conception of privacy Recital 26 merely recognises that it is impossible for them to exercise their rights once this happens.
2. Under the narrow conception of privacy, where data is obtained as personal data but is to be rendered anonymous before processing occurs, data subjects need not be informed of the purposes of processing that will occur only after anonymisation, even when this is known/envisaged[10]. On the other hand, under the broad conception of privacy, data subjects must be informed of the purposes of processing that will occur only after anonymisation when this is known/envisaged. In any event, data subjects must be informed of the intention to anonymise, the purposes of this, and the effects of it, which will not merely be to protect the identity of the data subject, but which will mean that thereafter the data subjects will not be able to exercise any control over the use of the data or information taken from it. (It needs to be emphasised that under the broad conception, anonymisation *of which the data subject is not informed*, in principle, threatens privacy rather than protecting it, because it results in the data subject losing all possibility of control of processing.)

---

[8] *R v Department of Health, Ex Parte Source Informatics Ltd* [2000] 1 All ER 786.

[9] See J Velu "The European Convention on Human Rights and the Right to Respect for Private Life, the Home and Communications" in A. H. Robertson ed. *Privacy and Human Rights* (Manchester: Manchester University Press, 1973) 12-128 at 92. See also, e.g., *P. G. and J. H. v the United Kingdom* (44787/98 [2001] ECHR 546 (25 September 2001), paragraph 56 and the further references given there.

[10] Although how this squares with the idea that anonymisation is itself a process under the Directive is not clear.

3. Under a narrow conception of privacy, where non-personal information is abstracted from personal data that is still held in personal form, the processing of the abstracted information is no longer the processing of personal data. Under the broad conception of privacy, the processing of information abstracted from personal data that is still held in personal form remains the responsibility of the person/s who holds the data in personal form. This person or persons must inform any persons to whom they disclose information (personal or otherwise) taken from personal data they hold of any restriction imposed on the use of the information, and these persons will be under a duty to observe these restrictions.

Because these issues significantly affect the objectives of the Directive at a fundamental level of conception, we recommend that

- **The Commission seek definitive clarification on these matters, if necessary from the European Court of Justice.**

Closely related to the definition of anonymisation as such is the definition of personal data. Member States' experience suggests that there is more ambiguity in the Directive's definition of personal data than might at first appear to be the case. For example, the UK maintains that data is personal if it the identity of the person can be identified directly by anyone or directly and indirectly by the data controller. In our opinion, there is no warrant for this, and it could restrict the application of the Directive in UK law in a way not intended by the Directive. For example, if Person A holds data in personal form by indirect identification but passes information contained within it to Person B who cannot identify the person to whom it relates directly or indirectly, who wishes to process it for purposes P (person B being the data controller for purposes P), then it is arguable under UK law, on the definition of personal data in the UK Data Protection Act 1998 alone, that the data protection principles do not apply to processing by Person B.[11] Contrary to this, other Member States interpret Recital 26 to indicate that information

[11] This said, it is arguable that processing by B is not outside the scope of the UK law on account of the provision that processing of personal data includes processing of information contained within the data unless the context otherwise dictates (see Section 1). However, this is contentious and has, arguably, been rejected by the UK Court of Appeal in *Source Informatics.* In any event, it makes the question depend on context in a way that the Directive does not appear to do. Alternatively, it could be argued that the processing by B falls under the Directive because any processing by B that A envisages is to be regarded as processing by A. However, this is contentious and the processing by B might not have been envisaged by A.

processed remains personal data if anyone can directly or indirectly identify the person to whom it relates.

Then there is the fact that the German law, for example, operates with an absolute conception of anonymisation, which means that data is treated as personal if it is at all possible that the data subject could be identified rather than if it is "reasonably likely" that identification could occur. Since Recital 26 clearly makes reference to "reasonable likelihood" this might reflect a particular interpretation of the force of Recitals in Germany, but this interpretation clearly places Germany outside the majority of Member States' understanding on this point. Finally, in the *Durant* case in the Court of Appeal of England and Wales, the Court has declared that personal data not processed in an automatic fashion are not in a filing system unless the file is structured so as to give as ready access to personal data within it as would be the case if the data were held in a computer. The Court further held that a file was not relevantly structured if it had to be read to find out what personal information it contained, and that a file catalogued under a person's name did not constitute such a file simply on account of this cataloguing. Because this appears to have the effect of placing almost all personal data processed by other than automated means outside the scope of the Directive, it is arguable that this is not the objective of the Directive.[12] In the *Durant* case, the UK Court of Appeal also gave a controversial interpretation of what it means for personal data to be data relating to an identified or identifiable person. The Court interpreted this narrowly, so that data relating to a complaint made by a person is not data relating to the person if it is not specifically data about what the person has done or other characteristics of the person.

We recommend, therefore, that

The Commission seeks to clarify:

a. **whether or not data remains personal if anyone can without unreasonable effort identify the persons concerned**[13]**;**
b. **more precisely what structuring is necessary for data to be held in a filing system (even though the Directive does in Recital 27 delegate this to Member States); and**
c. **the interpretation of "relating to" an identified or identifiable individual.**

[12] Indeed, we were unanimous that it is not.

[13] Those who adopt the broad concept of privacy believe that it does remain personal data.

(d) Recommendations around Exemption for Research

In various places, the Directive provides for exemptions from at least some requirements of the Directive for purposes of research and statistics.

We wish to make two recommendations. First,

- **The Commission should issue guidance on whether the exemptions for research (apart from the exemption constructed by appeal to Article 13.1) provide an exemption from the first data protection principle (that processing be lawful and fair).**

The group takes the unanimous view that the exemptions for research do not provide an exemption from the first data protection principle (unless an exemption is constructed by appeal to Article 13.1). Commonly, however, experience of REC members indicates that researchers are inclined to believe that once they fulfil exemptions for research that they are released of duties to provide information to the data subject. In the group's opinion, misunderstanding about this can arise by considering the conditions of Articles 7/8 to be sufficient for lawful processing, which they are not (see above). It can also arise from misunderstanding the implications of an overlap between the first data protection principle (that processing must be lawful and fair) (Article 6.1(a)) and the second data protection principle (that processing must be for specified and lawful purposes only and not performed in a manner incompatible with these purposes) (Article 6.1 (b)). The overlap arises because the requirement of fairness is partly articulated in Articles 10 and 11, which concern the duty to provide information to the data subject (which is also the concern of the first part of the second data protection principle). However, Article 6.1)(b) provides that further processing for historical, scientific (hence research), and statistical purposes are not to be regarded as incompatible with the purposes for which data was obtained (if appropriate safeguards are provided). Now, it might be tempting to infer that this means that research is to be regarded as a compatible purpose and also that the prohibition of Article 6.1(b) is on processing for incompatible purposes so that processing for compatible purposes is permitted under this Article. If so, an exemption in the terms of Article 6.1(b) will be readable as an exemption from the requirement to specify research purposes to the data subject (which will involve a partial exemption from requirements under the first data protection principle). We believe this to be an error, because the second data protection principle does not prohibit processing for incompatible purposes but processing for specified and lawful purposes in a manner incompatible with these purposes. Thus, that processing research might be considered not processing in a manner incompatible with the specified and lawful purposes does not mean that this processing is to be

considered processing for a specified and lawful purpose. In other words, the exemption does not exempt in relation to the first principle because it does not exempt in relation to the first part of the second principle. Interesting questions arise as to what exactly is meant by an incompatible/compatible purpose, and the Commission might wish to provide guidance on this for purposes of general implementation of the Directive. However, in our opinion it is not necessary, for present purposes, to speculate about this. In the context of PRIVIREAL, our view is that the effect of the second half of the second principle is to create a hurdle that processing must be passed and the exemption to that half for research indicates merely that for research (at any rate) under suitable safeguards this prohibition may be lifted.

It must be stressed that this is not a difficulty seen on the face of the Member States' laws, but is instead a problem of interpretation of those laws by researchers.

Finally an issue arises about the possible difference between "research for a historical purpose" and "historical research". Article 32.3 states that Member States may (under appropriate safeguards) exempt processing for the sole purpose of historical research altogether from Articles 6, 7 and 8. In effect, under appropriate safeguards, the provisions of the Directive do not apply. But, clearly, they do apply to processing for historical purposes, otherwise there is no need for reference to these in Articles 6.1(b) and (e). This raises the possibility that there might be a difference between "historical research" and "research for historical purposes", although it is difficult to draw such a distinction because of reference to "historical research" in Article 13.2. In our opinion, however, the key is whether or not the processing is solely for historical purposes/historical research or the data is held/processed for other purposes as well and it is this that differentiates the application of Article 32.3 from other provisions relating to historical research or use for historical purposes. Nevertheless, because questions have been raised about this matter, we recommend that

- **The Commission submit the issue to the Article 29 Working Party for guidance to clarify a possible difference between processing for historical purposes (see Articles 6.1(b) and (e)) and processing for historical research (see Articles 13.2 and 32.3).**

(e) Recommendation around "Explicit Consent"

Article 7(a) legitimates processing of personal data with the unambiguous consent of the data subject. Article 8.2(a) lifts the prohibition on the processing of special categories of data with the explicit consent of the data subject. However, Article 2(h) specifies that "the data subjects'" consent

means "any freely given specific and informed indication" by which the data subject signifies his/her agreement to the processing. This raises the question of the difference between unambiguous, signified, free and informed consent and explicit consent. Some Member States interpret explicit consent as written consent. However, in our opinion, verbal consent is no less explicit than written consent and the opposite of explicit consent is implicit consent. Implicit consent should, we suggest, be interpreted as any consent that is signified by an action from which consent may legitimately be inferred. For example, consent to having an injection may be inferred from a patient presenting his arm on being told that the doctor wishes to give him an injection. Consent to an action (A) may also be inferred from explicit consent to another action (B) where A is necessary to do B. However, simply failure to object is not to be interpreted as implicit consent because the failure to object is not to be regarded as an action by which agreement is signified. This is not because omissions are never to be considered actions, but because an action in response to something requires knowledge of what is being responded to, and failure to object may be the result of lack of knowledge of any choice in the matter. That said, a specific ticking of a box to signify that the data subject does not object is to be interpreted as at least implicit consent. This is not to say that written consent (or otherwise recorded or witnessed) is not important in medical research and other cases involving special categories of data. The difference between "explicit" and "implicit" consent is about whether or not an inference is required to conclude that consent has been given. Written consent is simply a matter of a matter of probity and evidence for which there can be other substitutes.

- **We recommend that the Commission issue guidance on the meaning of explicit consent, and further recommend that the general lines of the analysis we have presented here be adopted in this guidance.**

(f) Recommendations around data relating to dead people

The Directive is clear that it concerns the protection of natural persons, as opposed to legal persons (and Member States are free, therefore, to protect the personal data of legal persons as they see fit). Recital 2 requires data-processing systems, "whatever the nationality or residence of natural persons", to "respect their fundamental rights and freedoms"; Article 1.1 requires Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data; and Article 2 defines Data Subject as "an identified or identifiable natural person". What is left unclear is whether the rights extend to the living and the dead, or only to the living.

This is not a question of "rights" for the dead. The central issue is whether the Directive covers data that relates to a person who has died. It concerns whether duties apply to the personal data that was obtained from living people who are now dead. Clearly, some of the duties of the Directive do not apply. It is not possible to inform the dead person about the processing of the data or to seek their consent for new processing. However, if the data was collected from the dead person when alive for specific purposes, do duties in relation to the processing of that data continue for those stated aims? Must the processing remain lawful and fair? Must the data be kept securely? Is the effect of the death of the data subject that of removing the data from the scope of the Directive. The implementation of the Directive by Member States shows a variety of approaches to this area.

There are a number of reasons why it would be appropriate that those parts of the Directive that are capable of applying to the personal data of those who have died should do so. For example, even if the dead cannot enjoy rights for themselves (which is a controversial subject that raises questions of the concept of rights, amongst others, that we will not debate here):

- third parties (like relatives) should be able to control personal data relating to the dead person that the third parties have a legitimate interest in even though it is not personal data relating to themselves; and
- the use of personal data from the dead might need to be restricted in order to satisfy the legitimate expectations of living persons before they died.

Depending upon the particular issues raised, applications of the Directive might require powers to be given to interested third parties, agents of the dead person, or the Supervisory Authority.

- **We recommend that the Commission should seek to determine whether the dead are or are not be included within the definition of "natural person" in the Directive.**

(g) Recommendations around Prior Checking

Data protection hinges, to a very large extent, upon knowledge that processing is happening or that it is planned. A data subject only has effective rights when he or she has control of their data, which depends upon knowledge. The effective operation of the Directive, to a very large extent, relies upon being able to trust data controllers to notify the data subject and/or the Supervisory Authority of their intentions concerning the processing of data.

There is a general issue about the effectiveness of the registration procedure to ensure, where applicable, that all data controllers will register with the Supervisory Authority and comply with their duties. However, the issue of retaining control over one's data is challenged where data is anonymised and where Article 11 appeals to disproportionate effort and cost in order to gain an exemption form informing the data subject. Where data is collected directly from an individual, then knowledge of foreseen processing, the identity of the data controller, and other information, essential to making the judgement of whether to hand over one's data, is clearly available allowing the data subject to exercise personal responsibility towards the data. Where the data controller is in an Article 11 situation or has anonymised the data without retaining the codes (or even, perhaps, has gathered anonymous data having made certain representations as to processing), there is a very real possibility that the information will be processed without the data subject's knowledge or consent. As in the case of the duties relating to the personal data of the dead, there is a place for the protection of that data (and the protection of public confidence in the protection of personal data) through "prior checking" of proposed processing by Supervisory Authorities.

Article 18 provides that the Supervisory Authority shall be notified by data controllers of their processing of personal data (with limited exceptions). Article 20 establishes forms of prior checking. Member States must have in place a system for identifying processing operations that are "likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof", and may also check legislation. This is a powerful safeguard to ensure that where data subjects have lost the possibility of controlling their own personal data, the Supervisory Authority or an independent data protection officer will maintain a degree of protection over that data. It is clear from PRIVIREAL's work that the compulsory elements of this provision is not evenly applied, and that the potential of prior checking is not realised to protect data subjects in the majority of countries.

- **We recommend that the Commission issue guidance to encourage greater provision for and use of prior checking to ensure that Articles 18, 19, and 20 are given their full weight by Member States.**

Article 13.2 provides that "subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes

of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics". The issue here is again one of assessing the risk in the particular case. Again there is a clear need for prior checking to ensure that there is no risk to the data subject.

- **We recommend that the Commission should take steps to ensure that in relation to Article 13.2 prior checking be made explicit as part of the legislative measures and adequate legal safeguards to maintain the protection of the data subject.**

Further, Article 21 makes provision for publicity for processing operations, referring to the case of processing not subject to notification. Again, this provision could be used to raise the data subject's access to information about the processing of his/her personal data.

- **We recommend that the Commission give guidance to encourage Member States to use the publication of processing information in a way to make it more easily accessible to individual data subjects.**

(h) Recommendations concerning Article 13

Appeal to Article 13 gives Member States considerable powers to exempt processing from the provisions of the Directive. Recognising this, Article 28.4 grants anyone the right to have the lawfulness of an appeal to Article 13 checked by the Supervisory Authority. However, if this provision is to be effective, it requires application of the powers under Article 13 to be made explicitly.

- **We recommend that the Commission requires that Member States publish when they have used Article 13 to modify various applicable provisions in the Directive.**

(i) Recommendations around Third Country Data Transfers

The Directive is designed to enable personal data to flow unimpeded across national borders, based upon a principle of a minimum standard of protection. This is required of Member States, the EEA, and the NAS. Outside those allies, the principles remain the same—data can be transferred to countries granting equivalent protection or to companies contracting to grant equivalent protection or where "safe harbour" agreements apply.

The key difficulty here is not so much the slow development of agreements with countries and companies outside the EU and related areas, but the difficulties of intra-company transfer of data. There seems to be a degree of

uncertainty as to the position of the transfer of data from one office of an international company to another of its offices outside the protected area.

- **We recommend that the Commission give guidance to ensure that companies proposing a transfer of data between offices but not within the protected zone should register its procedures (e.g. staff training in Third Country offices) and safeguards for the data with Supervisory Authorities and the Commission, creating equivalent provisions as the safe harbour in the office or subsidiary/associate.**

(j) Recommendations concerning RECs and Data Protection in Medical Research

Many of the issues of the creation of RECs have become a requirement for Member States under the Clinical Trials Directive (2001/20/EC). This directive makes certain requirements but falls short in a number of respects identified as difficulties in the operation and constitution of RECs in PRIVIREAL Workshop 2. The Clinical Trials Directive gives an opportunity in its Article 8 to clarify the exact relationship between that Directive and the Data Protection Directive. The Article 29 Working Group could address these issues pursuant to that power.

- **We recommend that the Commission ensure that the implementation of the Clinical Trials Directive in relation to data protection in Member States' domestic law is monitored and analysed.**

However, Directive 2001/20/EC leaves certain matters of the constitution of RECs, identified as problematic in Workshop Two, without resolution. Central to this is the need to recognise that RECs are not *ad hoc* private groups but are public bodies issuing opinions and in some cases making decisions that carry out public policy. As such, they must be seen to display adherence to general principles of natural justice, human rights and the law generally. Thus, the nature of the membership of RECs is important, as is the methods of operation of the Committee. Further, while Directive 2001/20/EC indicates the need for independence of RECs it does not recognise fully the interests that can conflict, particularly the difficulty of placing a committee within a University or Hospital context for its accountability structure, when the outcome of the review is clearly of great economic interest to that body. Thus, legal expertise is needed to support the RECs. The discussion divided between those who feared a legal reductionism in the composition of RECs, and those who saw a potential conflict of interest in the provision of legal expertise to an REC from another body, for example a Ministry of Health or

Hospital. The majority felt that a legally qualified committee member could be a resolution of this problem of ensuring that legal data protection requirements are observed in research.

- **We recommend that the European Commission give serious consideration to the need for RECs to have:**
- **a standard membership balancing different commonly held ethical perspectives and other interest groups**
- **adequate legal and other expert resources to support their work**
- **full independence from conflicting interests and accountability as public bodies.**

A further inadequacy identified in the current REC structure was the problem of hierarchy of committees. It was widely reported that research teams could present the same protocol at a variety of committees in some States until they received a decision that was favourable. This indicates that there is a considerable lack of consistency in decision-making between RECs, and that while Directive 2001/20/EC imposes a duty to give reasons, the basis of decisions made varies widely between committees. Such a divergence of opinion would not be acceptable and needs to be addressed in the REC context. Further, an appeal, based upon errors should be introduced, rather than allowing "forum shopping".

- **We recommend that the Commission issue guidelines on the need for effective and transparent appeal structures from RECs, and that the Commission develop guidelines on good REC decision-making.**

The most difficult issue is the need for RECs to include in their scrutiny of the ethics of a proposal its legality (and in particular the legality of the protocol in relation to the Data Protection Directive). Directive 2001/20/EC requires that data protection rights be safeguarded for the human subjects of all clinical trials (Article 3.2(c)) (but the relationship of this provision to Articles 6.1 and 6.2 is unclear). This will be a considerable shift for some States' RECs. On the one hand, many members indicated a State position that required RECs to consider the law, others proscribed such consideration by RECs because of issues of support, competence and liability. Some States do not require RECs to assess the legality of a protocol because it is evaluated for that elsewhere. What is clear is that the assessment of the legality of a protocol is an essential protection for data subjects/research subjects as they do not necessarily know that the research is proposed. It is the same issue as prior checking and requires a full evaluation of the data protection rights of the research subject on behalf of or by the REC.

- **We recommend that the European Commission act to ensure that there is scrutiny of the legality of a protocol (specifically with regard to respect for the legal rights of research subjects) as part of that evaluation in all medical research proposals (especially as regards data protection rights);**
- **And (insofar as this is within the power of the Commission) that RECs should not be permitted to approve as ethical activities that involve violation of the legal rights of research participants.**

(k) Data Protection and Genetic Information

The problems for data protection raised by the use of genetic data were discussed at Workshop Three. A number of key issues were identified. If samples constitute personal data, then the Directive applies fully to them. However, it is arguable that they are not in themselves personal data, but only personal data when linked to other information relating to an individual. Much depends here on the precise interpretation of the Directive's definition of personal data. However, even if samples are never personal data, their processing raises issues analogous to those raised by the processing of personal data. Therefore, regulation on similar principles, or even the same principles, would be appropriate or even required. However, it was felt that there may be certain characteristics of genetic samples that would not be adequately protected by modelling regulation of the area on Data Protection alone.

The scope of the issues relating to the protection of genetic information is beyond the ambit of PRIVIREAL, which concerns data protection and medical research. The discussions identified a variety of different approaches and cultural positions, and this is reflected in the approaches in Member States' general laws. This raises issues beyond data protection alone, requiring detailed attention before data protection issues can be settled.

- **We recommend that the Commission fund an examination of these matters with emphasis on the broader context of genetic information in society.**

(l) Is there a Need for Special Instrument for Medical Research?

One way to clarify questions about the processing of personal data for research is for the EC to issue a special Directive or regulation in this area. However,

- **We recommend that a special data protection instrument for medical research is unnecessary and that sufficient clarification**

can be obtained by the Commission considering the questions we have posed and issuing appropriate guidance.