Chapter 2

An Overview of Directive 95/46/EC in Relation to Medical Research

Deryck Beyleveld[1]

Introduction

This chapter outlines the provisions of Directive 95/46/EC with the use of personal data for medical research centrally in mind. The Directive makes no specific mention of medical research and, consequently, it contains no provisions for medical research as an explicitly delineated category. However, at times, the Directive refers to medical purposes (though medical research is not explicitly listed under this category) and there are provisions relating to the use of data relating to a person's health. It also refers to the use of personal data for scientific research or statistics. Consequently, this overview is an analytic construction from these related provisions together with any other of the Directive's provisions that could apply to medical research, including those of a wholly general nature that apply to any processing of personal data.

The overview that follows represents my personal view, rather than the collective view of the participants in the PRIVIREAL project. It is presented here for the benefit of the general reader and also because it might assist in understanding the questions that participants were asked to address for the purpose of gathering the information for the comparative analysis presented in Chapters 10 and 11.

Objective of the Directive

The purpose of Directive 95/46/EC is to enable the free flow of personal data from one European Union (EU) Member State to another for the purposes of the internal market by ensuring that fundamental rights and freedoms of individuals (in particular, privacy) are safeguarded (see Recitals 3 and 10 and Article 1(1)) and a high level of equivalent protection of these rights and freedoms is ensured in all the Member States (see Recitals 7 and 8). The Directive gives substance to and amplifies the fundamental rights and freedoms contained in the Council of Europe

---

[1] Privireal Co-ordinator.

Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (see Recital 11). Since at least the *Second Nold Case (Case-4/73)* [1974] E.C.R. 507, the European Court of Justice (ECJ) has recognized, at least in principle, that violation of fundamental rights as fundamental principles of EC law (in which are included the fundamental rights and freedoms of the European Convention on Human Rights (ECHR) of the Council of Europe [which is alluded to in Recital 10]), is sufficient to invalidate at least *secondary* Community Acts.[2] However, despite the fact that a commitment to fundamental rights and freedoms has subsequently been enshrined in Article 6 of the Treaty of European Union (the 'Treaty of Maastricht'), it must not be forgotten that the EU does not have competence to legislate for fundamental rights and freedoms *for their own sakes*. The legal basis of EC law generally lies in the aim of constructing a single European market (and the legal basis of the Directive lies specifically in the aspect of the single market referred to as 'the internal market'). Thus, the competence of the EU to legislate to protect fundamental freedoms and rights only arises for the reason that this protection is deemed necessary for achieving the purposes of the single market. For this reason (as well as for the reason that the Directive is concerned in its attention to fundamental rights and freedoms not only to protect privacy but all fundamental rights and freedoms to the extent that they may be interfered with in the use of personal data)[3] it can be misleading to refer, as is often done, to the Directive as 'the Privacy Directive'.

Article 1(2) asserts that Member States shall not restrict or prohibit the free flow of personal data between themselves for reasons connected with the protection of fundamental rights and freedoms. However, this does not mean that the Directive is essentially concerned with legislating a balance between fundamental rights and freedoms and economic objectives of the internal market (let alone that the purpose of free flow between Member States overrides all considerations of fundamental rights and freedoms). Instead, adequate safeguarding of fundamental rights and freedoms must be viewed as a condition of the free flow of personal data, in line with which Article 1(2) signifies, primarily, that if a Member State (A) implements the Directive correctly then another Member State (B) may not restrict or prohibit the flow of personal data from B to A because B does not consider the level of protection for fundamental rights and freedoms provided by A's implementation to be adequate (see Recital 9). Presumably, it also means that if B does not consider that A provides the protection required by the Directive, then B may not restrict or prohibit the flow of personal

---

[2] Manfred A. Dauses, 'The Protection of Fundamental Rights in the Community Legal Order' (1985) 10 *European Law Review* 398–419, at 407, argues (on the basis of Articles 53 and 64 of the Vienna Convention on the Law of Treaties 1969, according to which any treaty is void if it violates a peremptory norm of general international law) that, in theory, violation of at least some fundamental rights is sufficient to invalidate even the European Treaty itself. However, it must be remembered that the ECJ has no jurisdiction to rule on the validity of the Treaty (see Article 234 EC (ex Article 177)).

[3] This is because the words 'in particular privacy' in Article 1(1) mean 'especially privacy' not 'only privacy'.

data from B to A on that ground either (but should refer the matter to the Commission or the ECJ). This, however, is not to say that the Directive is not concerned with a balance between economic objectives and the protection of fundamental rights and freedoms. However, such a balance is best viewed, in my opinion, as 'internal' to the activity of protecting fundamental rights and freedoms rather than as signifying a conflict between the protection of fundamental rights and freedoms as such and other factors. This is because to view the matter 'internally' is to observe that, e.g., Article 8(1) (the right to private and family life) of the ECHR may be derogated from in terms laid down by Article 8(2) ECHR, and relevant considerations include the economic well-being of the country, and may include economic objectives more generally to the extent that they serve, e.g., the fundamental rights and freedoms of others, or the public interest. To view the matter 'externally', on the other hand, requires the objectives of the internal market to be seen as in conflict with the entire framework set up by, e.g., Article 8(1) *together with* Article 8(2), which is both unnecessary and not consistent with the concept of a *fundamental* right or freedom.

Definition of Personal Data and Scope of the Directive

The Directive defines personal data as any information relating to an identified or identifiable natural person ('data subject') (see Article 2(a); Recital 26), and this includes 'sound and image data relating to natural persons' (see Recital 14). An identifiable person is, in turn, defined as a person who can be identified directly or indirectly from the data in conjunction with other factors (see Article 2(a)) 'likely reasonably to be used' by any person (see Recital 26—which also specifies that codes of conduct under Article 27 may provide guidance about when data have been rendered anonymous).

Recital 26 states that the principles of data protection (see below) apply to all personal data (within the scope of the Directive), but that they do not apply to data that have been rendered anonymous so as to render the data subject no longer identifiable (i.e. that has rendered the data non-personal). That data remains personal if *any person* is reasonably likely to be able to identify the data, seems to imply that data are not to be considered anonymous for the purposes of processing by a data controller (whom Article 2(d) defines as any person or body (private or public) that individually or jointly determines the purposes and means of processing) who cannot identify the data subject directly or indirectly from the data if any other person is reasonably likely to be able to identify the data subject directly or indirectly. If so, the circumstances in which data may be considered anonymous are extremely limited. However, precisely when data may be considered to be rendered anonymous and whether (and to what extent) processing of data in anonymous form that has been collected in personal form falls under the

Directive are highly controversial matters. (Anonymization is discussed in Chapter 4—and see also Deryck Beyleveld and David Townend 2004.[4])

'Natural person' is not defined. However, by stating that national legislation concerning the processing of personal data relating to legal persons is not affected by the Directive, Recital 24 suggests that a natural person is a person who is not a legal person. Processing of personal data covers anything that can be done with personal data automatically or manually (see Articles 2(b) and 3(1); Recital 27). However, the Directive only covers manual processing if the data are part of or intended to be part of a 'filing system' (see Article 3; Recital 15), which is defined as a 'structured set of personal data which are accessible according to specific criteria' (see Article 2(c); Recitals 15 and 27). Member States may define these criteria (see Recital 27). The Directive also does not cover processing of personal data for purposes that fall outside of the scope of EC law or processing by a natural person for purely personal or household purposes (see Article 3(2); Recitals 12, 13 and 16).

Situations in which Member States must apply their national law implementing the Directive are specified in Article 4 (and see Recitals 18–21).

Limits on Member States' Discretion in Implementing the Directive

Member States have a degree of discretion as to the conditions of lawful processing under national law. However, this discretion is limited by Articles 6–21, with which national laws must be compatible (see Article 5; Recital 22). Implementation may be by means of a general law or different laws for different types or 'sectors' of processing (see Recital 23).

Principles of Data Protection

Article 6(1) (see also Recital 28) lays down five principles of data protection, which are that personal data must be

- processed fairly and lawfully (see Article 6(1)(a));
- collected for specified, explicit and legitimate purposes (which, according to Recital 28, must be determined at the time of collection of the data) and not further processed in a way incompatible with those purposes (see Article 6(1)(b)) as originally specified (see Recital 28);
- adequate, relevant and not excessive in relation to the purposes for which they are collected/further processed (see Article 6(1)(c));

---

[4] Deryck Beyleveld and David Townend 'When is Personal Data Rendered Anonymous? Interpreting Recital 26 of Directive 95/46/EC' (2004) 6 *Medical Law International* 2: 73–86.

- accurate and, where necessary, kept complete and up to date (see Article 6(1)(d));
- not be kept in a personally identifiable form for longer than necessary for the purposes for which they were collected or (compatibly) further processed (see Article 6(1)(e)).

Article 6(2) requires Member States to impose responsibility for compliance with the data protection principles on the data controller (see also Recital 25).

Regarding the 2nd principle, further processing for historical, statistical and scientific purposes is not incompatible provided that Member States provide appropriate safeguards (see Article 6(1)(b)), which 'must, in particular, rule out the use of the data in support of measures or decisions regarding any particular individual' (see Recital 29). Regarding the 5th principle, for these purposes and under appropriate safeguards, personal data may be kept for longer than necessary for the purposes for which it was originally collected (see Article 6.1(e)).

The 1st principle can be viewed broadly or narrowly. Viewed broadly, for processing to be lawful, all the requirements of the Directive imposed on processing must be complied with. Thus viewed, compliance with the 2nd, 3rd, 4th and 5th principles is necessary to satisfy the 1st principle, as is compliance with Articles 7–21. Viewed narrowly, only some of the requirements for lawful processing under the Directive as a whole are requirements for lawful processing in relation to the 1st principle specifically, and the wording of Recitals 30–36 (in particular, Recital 31) suggests that these are the requirements of Articles 7 and 8, while Recital 38 suggests that the requirements of Articles 10 and 11 are the Directive's specific requirements of fair processing.

However, whichever way the matter is viewed, satisfaction of the conditions specified under Article 7 'Criteria for Making Data Processing Legitimate' and Article 8 'Special Categories of Processing' (see below), cannot be taken to be sufficient to render processing lawful under the Directive as a whole. Articles 6–21 all set (where applicable, given the nature of the personal data and processing, and taking into account exemptions) requirements that are hurdles to be overcome to render processing lawful. For processing to be lawful under the Directive as a whole, all the applicable hurdles must be overcome.

Necessary Conditions for Legitimate Processing of Personal Data and Sensitive Personal Data

Article 7 (see also Recital 30), which applies to all personal data, can be satisfied in six different ways

a. by obtaining the unambiguous consent of the data subject, 'consent' being defined by Article 2(h) as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'; or

b. if processing is necessary to perform or enter a contract to which the data subject is party; or
c. if processing is necessary to comply with a legal obligation of the data controller; or
d. if processing is necessary to protect the vital interests of the data subject (which Recital 31 reveals to be interests 'essential for the data subject's life'); or
e. if processing is necessary in the public interest or in the exercise of official authority (in relation to which Recital 32 states that national legislation may determine who the controller performing a task carried out in the public interest should be); or
f. if processing is in the legitimate interests of the controller or recipients of the data (unless protection of the fundamental rights and freedoms of the data subject is overriding) (with Recital 30 explaining that Member States may specify when this condition is satisfied).

With regard to Article 7(e) and 7(f) at least, Article 14(a) (see also Recital 45) specifies that these conditions may not be appealed to unless the data subject is given the opportunity to object on compelling legitimate grounds, *unless* 'otherwise provided by national legislation'.

Article 8 applies to what Recital 34 calls 'sensitive categories' of personal data, which Recital 33 characterizes as 'data which are capable by their nature of infringing fundamental freedoms or privacy'. Article 8 specifies such data as 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . data concerning health or sex life'. Article 8(1) *prohibits* the processing of such data, *unless* certain conditions are satisfied (see Article 8(2)(a)–(e) and 8(3)–8(5); and Recitals 33–36). For the purposes of processing data concerning health, the most relevant are

Article 8(2)(a) with the 'explicit consent' of the data subject (see also Recital 33) (which is not defined in the Directive) (unless national law does not permit the prohibition to be lifted by the data subject's consent); or

Article 8(2)(c) where processing is necessary to protect the vital interests of the data subject or another person where the data subject physically or legally cannot give consent; or

Article 8(2)(d) the processing is of data manifestly made public by the data subject or that is necessary to establish, exercise or defend a legal claim; or

Article 8(3) where the processing is necessary for the purposes of 'preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the

obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy' (see also Recital 33); or

Article 8(4) subject to suitable safeguards (which, according to Recital 34, must also be specific) specified by national law or the decision of the Supervisory Authority in the substantial public interest (which decisions must, per Article 8(6), be notified to the Commission) (with regard to which Recital 34 identifies scientific research and government statistics as an important reason of public interest that might justify processing of sensitive categories of data). (The concept of 'public interest' in the Directive is discussed in Chapter 7.)

Article 8(7) provides that Member States must determine when personal data may be processed employing a national identification number or any other identifier of general application.

Because Article 7 applies to all personal data, it is obvious that it is necessary for the processing of sensitive personal data that at least one condition from Article 7 as well as one condition from Article 8 be met. However, it is also obvious that meeting some of the conditions in Article 8 will automatically meet a condition in Article 7. So, for example, meeting the condition of explicit consent in Article 8 will also meet the condition of consent in Article 7.

Nothing in the Directive states explicitly that any condition in Article 7 takes priority over any other; and the same must be said about the conditions in Article 8(2). Nevertheless, it is arguable, at least where the processing of sensitive personal data is concerned, that the conditions in Article 8(2) and those in Article 7 are not entirely open alternatives. This is because the European Court of Human Rights (whose judgments, while not binding on the European Court of Justice, are taken very seriously by the latter) has ruled that to process sensitive personal data without consent is by the very nature of the case an interference with the right to private life under Article 8(1) of the ECHR.[5] Of course, interference with the right

---

[5] See the case of *M.S. v. Sweden* 28 EHRR 313, paragraphs 34–35:
'34. The applicant and the Commission, stressing that information of a private and sensitive nature had been disclosed without her consent to a certain number of people at the Office, maintained that the measure constituted an interference [with her right to private life under Article 8.1]'.
35. The Court notes that the medical records in question contained highly personal and sensitive data about the applicant, including information relating to an abortion. Although the records remained confidential, they had been disclosed to another public authority and therefore to a wider circle of public servants (see paragraphs 12–13 above). Moreover, whilst the information had been collected and stored at the clinic in connection with medical treatment, its subsequent communication had served a different purpose, namely to enable the Office to examine her compensation claim. It did not follow from the fact that she had sought treatment at the clinic that she would consent to the data being disclosed to the Office (see paragraph 10 above). Having regard to these considerations, the Court finds that the

to private life can be justified (as stated in Article 8(2) ECHR) if done in accordance with the law when 'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.[6] However, this implies that consent must be obtained unless to do so would be impracticable/involve disproportionate effort or be otherwise inappropriate (e.g., because to do so would threaten the overriding rights of others). Consequently, it is at least arguable (and seems to me to be the case) that satisfaction of the conditions laid down by Articles 7 and 8(2) in ways that do not involve the consent of the data subject at least implicitly (as is the case, e.g., with the condition of being for a contract binding on the data subject) requires the obtaining of consent to be impracticable, etc. Only in the case of Article 8(2)(c) does it seem to me that this complex requirement will be satisfied automatically.

Provisions Relating to Journalism, Art and Literary Expression

Article 9 (see also Recital 37) permits exemptions or derogations from the Directive's requirements for processing 'carried out solely for journalistic purposes or the purpose of artistic or literary expression' but only if this is necessary 'to reconcile the right to privacy with the rules governing freedom of expression'. The relevance of this to medical research should be extremely limited.

Duty to Provide Information to the Data Subject

As a means to the protection of data subjects' rights to fundamental rights and freedoms, the Directive grants data subjects specific rights. In my opinion, first and foremost amongst these are the rights to information specified in Articles 10 and 11 (see also Recitals 38–40), which Recital 38 refers to as conditions of fair processing, which links these Articles to the 1st data protection principle. Granted, the Directive does not describe the provisions of Articles 10 and 11 as *rights* of the data subject, but as duties of the data controller. However, because failure to carry out the applicable duty will interfere with the data subjects' specific rights, from a logical point of view these provisions may be characterized as rights, and the main effect of them being characterized as duties of the data controller is to indicate that the data controller's duty does not rest on the data subject making any claim: i.e., the information needs to be provided without the data subject having to make a request for it.

Article 10 (see also Recital 38) covers the case where data are being collected from the data subject, whereas Article 11 covers cases where the data have not

---

disclosure of the data by the clinic to the Office entailed an interference with the applicant's right to respect for private life guaranteed by paragraph 1 of Article 8.'

[6] As, indeed, the European Court of Human Rights found in *M.S. v Sweden*.

been obtained from the data subject. In both cases, the data controller or 'his representative' must provide the data subject with information (except where he already has it) about the identity of the data controller and his representative (if any). In the case of Article 10, the data subject must also be informed about the intended purposes of the processing, whereas in the case of Article 11, the data subject must be informed of the purposes for which data have been or are to be disclosed. In both cases, the data subject must be given any other information required for the processing to be fair. Examples are given. In both cases, the recipients or categories of recipients, and the existence of the right of access to and the right to rectify the data concerning the data subject (granted by Article 12) are mentioned. In the case of Article 11, the requirement to provide this information may be lifted, in particular for statistical purposes or purposes of historical or scientific research, if the provision of information would be impossible or involve disproportionate effort or if recording or disclosure of the data is expressly laid down by law (see also Recital 40), subject to Member States providing adequate safeguards. However, information provision that falls under Article 10 is not explicitly stated to be open to such derogation. While Recitals 38–40 are, at least at first sight, ambiguous as to whether the derogations specified in Recital 40 apply to both the Recital 39 case (obtaining from the data subject) and the Recital 39 case (other cases) or only to the Recital 39 case, the fact that these derogations are only mentioned in connection with Article 11 in the operative part of the Directive indicates strongly that they apply only to the Recital 39/Article 11 case.

It is not at all clear whether Article 10 covers the case of a person who obtained personal data from the data subject and now wishes to use the data for a purpose or to make disclosures that the data subject was not informed about at the time that the data were obtained. The case for saying that it does is that Recital 38 states that purposes must be specified at the time of collection. However, Recital 39 states that exemptions parallel to those provided by Article 11(2) to Article 11(1) apply to disclosures that were not anticipated at the time of the collection. This creates considerable difficulties of interpretation, which I discuss in Chapter 6.

The reason why Articles 10 and 11 are at the core of the protection provided by the Directive is not only that information about the identity of the data controller, etc., is needed for data subjects to be able to exercise the other specific rights that the Directive grants them. If consent of the data subject is, at least as a matter of first presumption, necessary to satisfy the Article 7/8(2) requirement for legitimate processing in connection with sensitive personal data, then, because consent must be informed, information provision is necessary to satisfy the Article 7/8(2) requirement as well.

Power to Exempt from Article 10 and Other Provisions via Article 13(1)

Although there is no derogation from Article 10 explicitly specified within Article 10, it should, however, be noted that Article 13(1) provides for derogation from Articles 6(1), 10, 11(1), 12, and 21 (which imposes a duty on Member States to

publicize processing operations) to the extent that this is necessary to safeguard various goals (e.g., national security, defence, the detection and prosecution of crime, taxation policy) that are beyond the remit of EC law (see also Recitals 43 and 44), or (Article 13(1)(g)) to protect the data subject or the rights and freedoms of others (see also Recital 42 in relation to the rights of Articles 10, 11 and 12). (Related to this, Recital 70 states that the Directive allows the principle of public access to official documents [which reflects the ECHR Article 10(1) right to freedom of expression, because this includes the freedom to receive information] to be taken into account when implementing the principles set out in the Directive.)

It is important to note, however, that Article 28(4) requires Member States to provide for each national Supervisory Authority to hear, in particular, 'claims for checks on the lawfulness of data processing lodged by any person when the national provisions pursuant to Article 13' of the Directive apply.

Data Subjects' Right of Access on Request

Article 12 (see also Recital 41) grants a 'right of access', which includes rights to obtain from the data controller

- confirmation as to whether or not data relating to him or her are being processed and, if so, information at least about the purposes of the processing, the categories of data being processed, and the recipients or categories of recipients to whom the data have been disclosed;
- intelligible communication of what data are being processed and about the source of this data;
- knowledge of the logic behind any automated processing at least if covered by Article 15(1);
- rectification, erasure or blocking of data if its processing does not comply with the Directive (especially on the grounds of inaccuracy or incompleteness);
- notification to third parties to whom data has been disclosed of the exercise of the last mentioned right (unless this is impossible or would involve disproportionate effort).

In relation to the modification of Article 12 permitted by Article 13(1)(g), Recital 42 specifically indicates that Member States may require the data subject's right of access to medical data to be exercised only through a health professional. Article 12 is also subject to derogation via Article 13(2) 'when data are processed solely for the purposes of scientific research or are kept in personal form for a period that does not exceed the period necessary for the sole purpose of creating statistics', provided that

- the derogation is by a legislative measure;
- 'there is clearly no risk of breaching the privacy of the data subject'; and

- adequate legal safeguards are provided (in particular that the data are not used to take measures or decisions regarding any particular individual).

Data Subjects' Rights to Object

Article 14(a) grants a right to object to processing on legitimate grounds (as already mentioned in connection with Article 7) and Article 14(b) grants a right to object to processing for the purposes of direct marketing. Whereas the Article 14(a) right may be removed by national legislation, the Article 14(b) may not and data subjects must be informed of this right (the exercise of which must be free of charge and [see Recital 30] does not require reasons to be given) either whenever the data controller envisages the data being processed for direct marketing or before such processing or disclosure to third parties for such processing occurs.

Data Subjects' Right to Object to Decisions Based Solely on Automated Processing

Article 15 (as already alluded to in connection with Article 12) grants data subjects a right not to be subjected to decisions that produce legal effects on them or otherwise significantly affect them, which are based solely on automated processing that is intended to evaluate personal aspects of the data subject (unless certain conditions are satisfied).

Powers to Exempt for Research

The extent to which the Directive permits Member States to exempt medical research from various requirements set by the Directive is (as a category of scientific research/use for statistics) specified at least by Article 13(2), together with Articles 6(1)(b), 6(1)(e), and 8(4) (given that Recital 34 specifies scientific research, amongst other things, is an important public interest). In addition, where processing was already under way before the Directive entered into force (24 October 1998), Article 32(3) permits Member States to provide, on condition that they institute appropriate safeguards, that the processing of data for the sole purpose of 'historical research' (which category is not defined, in particular in relation to research for historical purposes, which is mentioned in Article 6(1)(b)) need not comply with Articles 6, 7 and 8. To this might possibly be added the derogations permitted under Article 8(3) (but only to the extent that medical research may be considered to be a subcategory of preventive medicine, medical diagnosis, the provision of care or treatment, or management of health-care services) and the derogation under Article 13(1)(g) (but only to the extent that medical research is necessary to safeguard the data subject or the rights and freedoms of others). (The power to exempt for research is discussed in Chapter 5.)

Need for Processing to Have the Consent of the Data Controller

According to Article 16, those who are authorized by the data controller to hold or otherwise process data must do so only on the instructions of the data controller unless required to do so by law. (See also Article 17(3), which further specifies that processors who are not themselves the data controllers must be bound by a contract or legal act binding them to the controller. Per Article 17(4), the contract must be in writing or equivalent form.)

Security

Article 17(1) and (2) (see also Recital 46) further requires Member States to provide that the data controller must implement appropriate security measures.

Notification to the Supervisory Authority

Article 18 concerns notification of processing to the Supervisory Authority that must be set up under Article 28 (see also Recitals 48–52). Article 18(1) requires Member States to require the data controller (or his representative) to notify the Supervisory Authority before carrying out any automatic or partly automatic processing. Article 18(5) permits Member States to require notification to the Supervisory Authority of non-automatic processing. Article 18(2) and (3) permits Member States to simplify or exempt from notification (the contents of which are specified by Article 19) under specified conditions, the most important of which where data processed for medical research is concerned is that the data controller, operating in compliance with national law, appoints a personal data protection official who is responsible, in particular, for ensuring in an independent manner the application of national provisions implementing the Directive and for keeping a register of processing operations as required by Article 21(2). Recital 51, importantly, specifies that simplification or exemption from notification does not exempt the data controller from any of the other obligations resulting form the Directive.

In addition to information about the identity of the data controller, the purposes of processing, data subjects, categories of data processed and recipients of data, Article 19(1) requires information about proposed transfers of data to countries outside the European Economic Area (EEA) (which is the EU plus Iceland, Lichtenstein and Norway) and a general description of a preliminary assessment of the security measures required under Article 17.

Requirement for Prior Checking of Processing Presenting Specific Risks to Rights and Freedoms of the Data Subject

Article 20(1) and (2) requires Member States to determine which processing operations are likely to present specific risks to the rights and freedoms of data subjects (about which Recital 53 provides some examples) and to subject these to prior checking by the Supervisory Authority or a Data Protection Official (who must consult the Supervisory Authority if in any doubt), and Article 20(3) permits member States to carry out such checks when preparing legislation that lays down appropriate safeguards for such processing operations. (See also Recital 54.)

Requirement to Publicize Processing Operations

Except in the case of public registers, Article 21 requires Member States to take measures to publicize all processing operations. For processing that requires notification per Article 18, a register must be kept by the Supervisory Authority that contains all the information required per Article 19(1) except that concerning a description of a preliminary assessment. Where notification is not required, Member States must ensure that this same information is available to any person on request.

Requirement to Provide Compensation for Damage Caused by Unlawful Processing

The Directive requires Member States, without prejudice to any administrative remedy, to provide for a judicial remedy for any breach of rights guaranteed by implementing national legislation (Article 22); to provide for compensation from the data controller for damage as a result of unlawful processing operations (except where the controller can prove that he was not responsible for the event causing the damage) (Article 23); and to adopt suitable measures to ensure full implementation of the provisions of the Directive, which must include sanctions for infringing these provisions (Article 24). (See also Recital 55.)

Transfer of Personal Data Outside the EEA

Articles 25 and 26 concern transfer of personal data to 'third countries' (i.e., countries outside the EEA). Personal data may not be transferred to a third country that does not provide for an adequate level of protection (Article 25(1); Recitals 56 and 57) unless with the unambiguous consent of the data subject; or when necessary for the performance of contractual measures between the data controller and the data subject, or at the data subject's request; or in the interest of the data subject in a contract between the controller and a third party; or when necessary or legally required on important public interest grounds or to exercise or defend legal

claims; or when necessary in the vital interests of the data subject; or from a public register (Article 26(1); Recital 58). Alternatively, Member States may authorize transfers where the data controller adduces adequate safeguards by e.g., appropriate contracts (Article 26(2); Recital 59), in relation to which the Commission may, in accordance with Article 31(2), decide that certain standard contractual clauses constitute sufficient safeguards, with which Member States must comply (Article 26(4)). Article 25(2) specifies considerations that Member States must take into account in assessing the adequacy of protection in a third country. Member States and the Commission must inform each other of countries they consider do not provide adequate protection (Article 25(3)). If the Commission does not consider protection in a third country to be adequate, Member States must act to prevent transfers of data of the type for which protection is not adequate to that country (Article 25(4)), while the Commission must act to try to remedy this situation (Article 25(5); Recital 59). The Commission may find, in accordance with Article 31(2), that a third country provides adequate protection, and then the Member States must comply with this decision (Article 25(6)). These matters are of special relevance in the case of personal data processed for medical research, because this research is often sponsored by companies based outside of the EEA, and, as Recital 60 indicates, non-compliance with the standards set by Article 8 of the Directive (which deals with sensitive personal data specifically) is of particular concern in relation to third countries. (As regards the powers of the Commission with regard to the transfer of data to third countries, see Recital 66, which makes reference to Council Decision 87/373/EEC.)

Codes of Conduct

Article 27(1) (see also Recital 61) requires Member States and the Commission to encourage the drawing up of codes of conduct to assist with the implementation of the Directive in specific sectors of processing. The Supervisory Authority is required to vet codes drawn up by bodies representing categories of data controllers and to consult with data subjects or their representatives (Article 27.2). Article 27(3) provides a role for the Article 29 Working Party in approving draft Community Codes and amendments to existing Community codes.

Requirement for and Role of a Supervisory Authority

Article 28 requires each Member State to provide for one or more public authorities ('the Supervisory Authority'), which must act in complete independence (see also Recital 62), and which (see also Recitals 63 and 64)

- is responsible for monitoring compliance with national measures implementing the Directive (Article 28(1));

- must be consulted when administrative and regulatory measures to implement the Directive are drawn up (Article 28(2));
- must be given investigative powers, effective powers of intervention, and the power to engage in legal proceedings regarding violations of the national implementing laws (the exercise of which powers may, however, be appealed through the courts) (Article 28(3));
- must hear claims lodged by any data subject or association representing a data subject, and when Member States are employing their powers under Article 13 must hear claims for checks on lawfulness of processing lodged by *any person* (in relation to which they must at least inform the person that a check has taken place) (Article 28(4));
- must draw up and publish a regular report on its activities (Article 28(5));
- may be asked to exercise its powers by the Authority of another Member State and must co-operate with the Supervisory Authorities in the other Member States insofar as this is necessary for it to carry out its duties (Article 28(6)).

The staff of the Supervisory Authority must be made subject to a duty of professional secrecy with regard to confidential information, which must continue after they have ceased to be employed by the authority (Article 28(7)).

Article 29 Working Party

Article 29 (see also Recital 65) sets up an advisory, independent, Working Party on the Protection of Individuals with respect to the Processing of Personal Data, and specifies the composition and *modus operandi* of the Working Party. The remit of the Working Party is (see Article 30(1); Recital 65) to

- examine any question concerning proper implementation of the Directive in relation to contributing to the Directives aim of ensuring harmonized protection within the EU;
- provide an opinion to the Commission on the level of protection in third countries;
- advise the Commission on any proposed amendments to the Directive or additional proposed Community measures affecting the rights and freedoms of individuals with respect to the processing of personal data; and
- give opinions on codes of conduct drawn up at Community level.

The Working Party's findings on any lack of harmonization must be reported to the Commission (Article 30(2)), and the Working Party may make recommendations on its own initiative (Article 30(3)). The Working Party's opinions and recommendations must be forwarded to the Commission and the Article 31 Committee (Article 30(4)). The Commission must make a report on action it takes on any of these opinions or recommendations to the Working Party, the European Parliament and the Council (Article 30(5)), which must be made public. Finally, the Working Party must make an annual report to the European Parliament and the

Council on the level of protection in Member States and third countries, which must be made public (Article 30(6)).

Article 31 Committee

Article 31 provides that the Commission is to be assisted by a Committee when it proposes to take Community measures. If the Committee agrees (by a majority in accordance with Article 148(2) of the European Treaty) to the measures proposed, they apply immediately. Otherwise, the Commission must submit the measures to the Council (which has 3 months to take a different decision by a qualified majority). It seems from Recital 68 that one of the specific purposes of Article 31 is to enable the Commission to supplement or clarify the principles of the Directive by making specific rules based on those principles for specific sectors. Thus, for example, it is possible, in principle, that the Commission might use Article 31 to implement specific community measures for the use of personal data for medical research.

Deadlines for Implementation and Powers to Make Transitional Exemptions

Article 32(1) requires Member States to have implemented the Directive within 3 years of its adoption (which was on 24 October 1995, hence by 24 October 1998). According to Article 32(2), by 24 October 2001, all processing already underway by 24 October 1998 must comply with the provisions of the Directive, except that Member States may delay conformity with Articles 6, 7 and 8 until 24 October 2007 in the case of processing of data already held in manual filing systems on 24 October 1998. (This implies that data can be subject to processing already underway when it is not already held; but this is not explained. In relation to medical research, one possibility is that data collected from a person after 23 October 1998, thus not held on 24 October 1998, for a project that began processing data on other persons before 24 October 1998, is to be considered being subject to processing already under way by 24 October 1998; but other interpretations may be possible.) This transitional exemption does not, however, extend to the rights under Article 12. (However, according to Recital 69, if data kept in existing manual filing systems is processed during the extended transition period applicable to them, 'those systems must be brought into conformity with these provisions at the time of such processing'.) According to Article 32(3), subject to the provision of suitable safeguards, Member States may permanently exempt data already held in manual filing systems before 24 October 1998 from Articles 6, 7 and 8, where the data are kept for the sole purpose of historical research.

Review of the Directive by the Commission

Article 33 requires the Commission to report to the Council and the European Parliament on the implementation of the Directive at regular intervals, beginning no later than 24 October 2001, and the reports must be made public. It requires the Commission, in particular, to keep under review the application of the Directive to the processing of sound and image data relating to natural persons and to submit any proposals that are rendered necessary by advances in information technology.

Responsibility to Implement the Directive

Article 34 addresses the Directive to the Member States. All EC Directives (as against EC Regulations) require implementation by the Member States and do not generally impose duties directly on private persons or bodies. However, under the doctrine of direct effect developed by the ECJ, once the deadline for implementation has passed, provisions of a Directive that are sufficiently clear and unambiguous to be applied directly by the domestic courts apply directly in the absence of implementing legislation and take precedence over any conflicting legislation.[7] If the domestic courts refuse to apply such provisions directly,[8] then the Member States are liable to penalties.[9]

---

[7] See, e.g., the second *Simmenthal* case, Case 106/77, [1978] E.C.R 629.
[8] That they are required to do so, at least if possible, was established in *Von Colson and Kamann v. Land Nordrhein-Westfalen* (Case 14/83) [1984] E.C.R. 1891.
[9] See *Wagner Miret v. Fondo de Guarantia Salaria* (C-334/92), [1993] E.C.R. I-6911.