Chapter 3
International documents on data protection

Contents

1 INTRODUCTION

By the 1980s, it had been recognised that data protection was a problem at more than the national level.[1] The global market had emerged, leading to an increased need for the exchange of information across national boundaries.[2] International organisations such as the Organisation for Economic Co-operation and Development (OECD), the European Council and the European Economic Community realised on the one hand that if multinational corporations were expected to conform to differing standards of data protection in every country in which they processed or stored data this would impose an onerous burden on them. On the other hand, they wanted to avoid the creation of data havens (countries where no data protection regulations exist) which could nullify other countries' efforts to protect their citizens' liberties.[3]

---

1 General international cooperation can be said to have begun in Teheran in 1968 with the International Conference on Human Rights. The broad issue was the protection of human values in the context of rapid technological progress. A United Nations resolution of 1968 (United Nations, Doc A/7218 (1969) 54) also drew attention to respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques. One of the first international discussions on privacy took place in Scandinavia in 1976 at a meeting of the International Commission of Jurists. The conference recognised that the right to privacy was of paramount importance to human happiness and recommended that all countries should take appropriate measures to protect privacy in all its different aspects. The Nordic Council (consisting of representatives from Denmark, Iceland, Norway, Sweden and Finland) recommended in 1971 that all Nordic governments should establish uniform data protection measures. Since the 1970s a host of international groups have been involved with data protection, *inter alia* the International Telecommunications Union, the Intergovernmental Bureau of Informatics, the United Nations Centre on Transnational Corporations, the European Community, the International Federation for Information Processing, the European Computer Manufacturers Association and the International Institute of Administrative Sciences (see Hondius *Emerging data protection* 55–79; Bennett *Regulating privacy* 131–133).

2 See Hondius *Emerging data protection* 242; OECD Guidelines 18; Blume 1992 *Computer/L J* 399, 403. Transborder data flows involve more than the issue of data protection. Business interests, such as interests in the export of products and services, are also involved and should also be catered for (see Bothe 1989 *Mich J Int L* 333).

3 Lloyd *Information technology law* 44; Walden "Data protection" 445. There are also commentators who are sceptical of the professed aim of data protection, namely to protect privacy, and who argue that these laws "are effective non-tariff barriers to the free flow of commercial and other information" (see Pinegar 1984 *Int Bus L'yer* 183, 187. See also McKeaver 1984 *Int Bus L'yer* 159; Schlundt 1985 *Inf Age* 67, 68). It would

(continued...)

During this period, two significant international documents or sets of rules concerning data protection were issued. The first was issued by the European Council and took the form of a Convention, namely the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[4] (the Convention). The second set of rules was Guidelines issued by the Committee of Ministers of the OECD called Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[5] (the OECD Guidelines). The purpose of these documents was twofold, namely to set standards for data protection at the national level, and to ensure the free flow of data at the international level.[6] In order to achieve these goals, these documents aimed to bring about equivalence[7] between national rules on data protection.[8] However, the two organisations approached the issue from different perspectives,[9]

3(...continued)
seem as if especially in the USA there is a suspicion that Europe is using data protection legislation as a pretext for economic protectionism (see Lloyd *Information technology law* 48).

4 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg 28 Jan 1981 (No 108/1981).

5 Reproduced in a booklet entitled Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1981), which will hereafter be referred to and cited as "OECD Guidelines". The booklet also contains an Explanatory Memorandum to the OECD Guidelines, which will hereafter be cited as "OECD Guidelines Explanatory Memorandum".

6 These two goals are in competition, and sometimes even in conflict, with each other. Data protection entails that an individual's personal information be kept confidential, *inter alia* by restricting the dissemination of such information. However, this can hinder the free flow of information. See also Beling 1983 *Boston College Int & Comp L R* 591, 594; Bing 1984 *Michigan Yb Int Legal S* 271, 273.

7 However, as Blume 1992 *Computer/L J* 399, 403 points out, an important policy problem is to understand what equivalence means. Is it sufficient that the same principles are followed in different countries, or should these principles be implemented in the same way? Part of this problem is whether countries should be allowed to categorise sensitive data differently. Blume argues (404) that a totally open market presupposes that a harmonised regulation should be achieved if the legal protection of citizens is to be taken seriously. He also points out, however, that different legal and political traditions can make this goal almost impossible unless binding international cooperation exists.

8 If different countries provide an equivalent level of data protection, information can be passed between them without impediments, since there is no increase in the threat posed to the privacy of individuals whose personal information is involved in the data transfer.

9 The two documents nevertheless resemble one another closely, which is to be expected since the Convention and the OECD Guidelines were formulated and discussed during the same period and to a large extent by the same countries. The two organisations also cooperated closely and strove to eliminate unnecessary differences between the two texts. See Hondius 1983 *Neth Int L R* 103, 113; Frosini 1987 *Computer L & Prac* 84, 87.

which is a reflection of the different purposes of the two organisations.[10]

These two documents preceded another very important document, namely the European Union's Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data[11] (the Directive), which is at present the most prominent document in the data protection arena.[12]

These three documents are by no means the only international documents that influence data protection – other documents include the United Nations' Guidelines Concerning Computerized Personal Data Files,[13] documents produced by the International Working Group on Data Protection and Telecommunications,[14] Amnesty International's Policy with Regard to Data Protection[15] and the Schengen

10 The Council of Europe has traditionally been a human rights organisation, and is also in charge of the European Convention of Human Rights (Blume 1992 *Computer/L J* 399, 405). It is therefore to be expected that the Convention will focus on the human rights aspect of the privacy concept. The OECD Guidelines on the other hand focus on the impact of data protection on international trade and economic development (see fn 18) (see also Bing 1984 *Michigan Yb Int Legal S* 271, 272; Hondius *Emerging data protection* 1983 *Neth Int L R* 103, 106).

11 1995 *Official Journal* L 281/31. See also fn 224.

12 Hondius 1983 *Neth Int L R* 103, 113 explains the relationship between the OECD, the European Council and the EEC (forerunner of the EU) by comparing it to concentric circles:

> The outer circle encompasses the OECD member countries. The Council of Europe members constitute the middle circle, and within the latter a group of ten States forms the inner circle, the EEC. The wider the circle, the more general and less binding the rules.

13 It was adopted in 1990 by the United Nations General Assembly, and gives member states "orientations" to follow when implementing regulations concerning computerised personal data files. It sets out ten principles concerning the minimum guarantees that should be provided in national legislation, that relate to (i) lawfulness and fairness; (ii) accuracy (iii) purpose specification; (iv) interested person access; (v) non-discrimination; (vi) power to make exceptions; (vii) security; (viii) supervision and sanctions; (ix) transborder data flows; and (x) field of application. (It can be found on the *Datenschutz* webpage at http://www.datenschutz-berlin.de/.) Also see Bennet *Regulating privacy* 250; Walden "Data protection" 447.

14 Eg, Telecommunications and Privacy in Labour Relations (1989); Report and Guidance on Data Protection and Privacy on the Internet (1996); Common Statement on Cryptography (1997), Common Position on Public Accountability in Relation to Interception of Private Communications (1998); Common position relating to Reverse Directories (1998); Common Position on Data Protection and Search Engines on the Internet (1998); Common Position on Essentials for Privacy-enhancing Technologies (eg P3P) on the WorldWideWeb (1998). All these documents can be found on the Internet at http://www.datenschutz-berlin.de.

15 Madsen *Personal data protection* 1001–1004.

Agreement.[16] However, the OECD Guidelines, the European Council's Convention and the EU Directive are at present the most widely followed and influential of the documents. This chapter will therefore confine itself to a detailed discussion of these three documents.

2 OECD GUIDELINES

2.1 Introduction

The OECD is a world-wide organisation of 29 countries[17] sharing the principles of market economy, pluralist democracy and respect for human rights.[18] The OECD established its first expert group on data protection, known as the Data Bank Panel, in 1969.[19] This panel examined the privacy issues

16 The Schengen agreement of 1985 eliminates border controls between France, Germany and the Benelux countries. It established a Schengen Information System for the exchange of information on population movement between the five countries (see Bennett *Regulating privacy* 249). The Schengen agreement was concluded in secrecy, and the data protection commissions of the three member countries who at that stage had data protection laws, ie Germany, France and Luxembourg, were only informed about it after the fact (Madsen *Personal data protection* 28). For a critical discussion of the problems posed by the Schengen agreement to data protection, see Shiraz 1995 *Int J Refugee L* 179–200. Also see Dumortier 1997 *Int R L Computers & Tech* 93.

17 Austria, Australia, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States of America (see the OECD website at http://www.oecd.org); Franklin *Business guide* 553 fn 1.

18 The OECD was preceded by the Organisation of European Economic Co-operation (OEEC). The OEEC was established in 1948 after World War II to administer American and Canadian aid under the Marshall Plan for the reconstruction of Europe. In 1961 the OEEC became the OECD under a Convention signed in Paris. Since then its vocation has been to build strong economies in its member countries, improve efficiency, hone market systems, expand free trade and contribute to development in both industrialised and developing countries (Archer & Butler *European Community* 8). Also see Hondius *Emerging data protection* 57; Beling 1983 *Boston College Int & Comp L R* 591, 593 fn 24.

19 OECD member countries meet and exchange information in committees. The overriding committee or supreme body is the Council. Each member country is represented on the Council. It also has an Executive Committee. Exchanges between OECD governments flow from information and analysis provided by a secretariat in Paris. The ICCP (Information, Computer and Communications Policy) committee of the OECD takes a special interest in data protection issues.

associated with digital personal information.[20] It held a seminar in 1974[21] where experts from most OECD member countries exchanged views on data protection issues, and another in 1977 in Vienna.[22] In 1978 an *ad hoc* expert group on data protection, called the Group of Experts on Transborder Data Barriers and Privacy Protection, was established. It was instructed by the Council of the OECD to develop a set of guidelines on personal data protection and transborder data flow. This resulted in the development of the OECD Guidelines over a period of three years.[23] These guidelines were finally adopted on 23 September 1981.[24] The OECD Guidelines were open for adoption by all companies and organisations in the member countries.[25]

2.2 Provisions of OECD Guidelines[26]

2.2.1 Nature of OECD Guidelines

It should be remembered that the OECD Guidelines are not legally binding – they are merely recommendations made by the OECD to its member countries regarding the adoption of good data protection practices in order to prevent unnecessary restrictions on transborder data flows.[27] Furthermore, they are formulated in general terms and it is generally expected of the member countries to work

20 Madsen *Personal data protection* 25.

21 OECD *Policy issues in data protection*.

22 This seminar was entitled *Transborder data flows and the protection of privacy* (see Bennett *Regulating privacy* 136–137).

23 It was developed by legal experts under the leadership of the Chairman of the Australian Law Reform Commission, Justice Michael Kirby (see Madsen *Personal data protection* 24; Bing 1984 *Michigan Yb Int Legal S* 271, 272.)

24 See fn 5.

25 In other words, countries did not have to join as a country. Eg, the USA did not sign the OECD Guidelines, but several hundred USA firms did sign it. However, according to commentators, few actually adopted the OECD Guidelines in practice (Madsen *Personal data protection* 25; Banisar *Privacy and human rights* 235).

26 For a discussion of the OECD Guidelines, see Beling 1983 *Boston College Int & Comp L R* 591, 603–618; Bing 1984 *Michigan Yb Int Legal S* 271–303.

27 See Walden "Data protection" 447.

out the details in their own national laws.[28] The OECD Guidelines set minimum standards which may be supplemented by additional measures. The OECD Guidelines do not require legislation for their implementation.[29]

2.2.2 Overview of structure of OECD Guidelines

The OECD Guidelines are divided into five parts. The first part explains the scope of the OECD Guidelines, contains definitions, and also explains that the OECD Guidelines should be regarded as minimum standards which should be supplemented by additional measures to protect privacy and individual liberties.[30] Part 2 contains eight basic principles relating to the protection of privacy and individual liberties at the national level.[31] Part 3 deals with principles of international application. These principles are concerned with the relationship between member countries, and involve the free flow of data and the issue of precisely when restrictions may legitimately be imposed.[32] Part 4 sets out how the basic principles should be implemented at the national level, specifying that they should be applied in a nondiscriminatory fashion.[33] Part 5 discusses international cooperation between OECD member countries and refers to the issue of conflict of laws which may arise when the flow of data involves several member countries.

2.2.3 Purpose of OECD Guidelines

28 Some of the OECD Guidelines are more detailed than others. Eg, the individual participation principle (see par 2.2.5.7) was spelled out in much more detail than the issue of choice of law (see fn 104). The level of detail depended on the extent of the consensus that could be reached on the resolutions and on the available experience and knowledge. It was consequently envisaged that the OECD Guidelines should constantly be reviewed and adjusted (OECD Guidelines Explanatory Memorandum 23).

29 See fn 86 and accompanying text.

30 OECD Guidelines par 1–6. On the meaning of individual liberties, see fn 34.

31 OECD Guidelines par 7–14.

32 OECD Guidelines par 15–18.

33 OECD Guidelines par 19.

The purpose of the OECD Guidelines is to balance the protection of privacy and individual liberties[34] against the advancement of the free flow of personal data[35] across national boundaries.[36]

The objectives of the OECD Guidelines can be stated as follows:

- achieving acceptance by member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data

- reducing differences between relevant domestic rules and practices of member countries to a minimum

- ensuring that in protecting personal data consideration is given to the interests of other member countries and the need to avoid undue interference with the flows of personal data between member countries

- eliminating, as far as possible, reasons which might induce member countries to restrict

---

34 The Group of Experts who drafted the OECD Guidelines preferred to use the concept "privacy and individual liberties" rather than the traditional concept of "privacy", which only relates to keeping personal data confidential, because other related interests, such as the obligations of record-keepers to inform the general public about activities concerned with the processing of data, and the rights of data subjects to have data related to them supplemented or amended, can also be identified in this area:

> Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

(OECD Guidelines Explanatory Memorandum 16).

35 It is important to remember that the OECD Guidelines attempt to balance two essential values, namely the protection of privacy and individual liberties on the one hand, and the advancement of the free flow of personal data on the other (see fn 6 and accompanying text). While the OECD Guidelines accept the need for certain restrictions to free transborder flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries (OECD Guidelines Explanatory Memorandum 22–23). Also see Madsen *Personal data protection* 24.

36 Transborder flows of personal data are defined as "movements of personal data across national borders" (OECD Guidelines par 1(c)). This definition restricts the application of certain provisions of the OECD Guidelines to international data flows and consequently does not deal with data flows within federal states. The definition includes the movement of data through electronic transmission, via satellite or any other means (OECD Guidelines Explanatory Memorandum 26).

transborder flows of data because of the possible risks associated with such flows[37]

2.2.4 Scope of OECD Guidelines

The OECD Guidelines apply to **personal data**, in the **public** or **private sector**, which, because of the manner in which they are processed by a **data controller**, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.[38]

The OECD Guidelines are based on the concept of "personal data" and not, as many national laws and the Convention are, on the concept of a "personal data system".[39] However, the OECD Guidelines also presume some structuring of the data, and do not apply to a single data element.[40] **"Personal data"** are defined as any information relating to an identified or identifiable individual.[41] In other words, data are "personal" if they may be connected to a particular physical person by direct (for example a civil registration number) or indirect (for example an address) linkages.[42]

The terms "personal data" and "data subject" serve to underscore the fact that the OECD Guidelines are concerned with natural (as opposed to juristic) persons. In other words, the OECD Guidelines recognise only **natural persons** as data subjects, and therefore do not protect the data relating to

37 OECD Guidelines Explanatory Memorandum 22.

38 OECD Guidelines par 2.

39 See eg the US Privacy Act which is based on a "system of records" (ch 2 par 4.2.2.3) or the UK Data Protection Act) which regulates the processing of data (ch 4 par 4.3.3.1), and on the Convention, see par 3.2.3. See also Bing 1984 *Michigan Yb Int Legal S* 271, 273.

40 In the Explanatory Memorandum to the OECD Guidelines it is stated that "the OECD Guidelines deal with the building-up and use of aggregates of data which are organised for retrieval, decision-making, research, surveys and similar purposes..." (OECD Guidelines Explanatory Memorandum 25). See also Bing 1984 *Michigan Yb Int Legal S* 271, 273.

41 OECD Guidelines par 1(b).

42 OECD Guidelines Explanatory Memorandum 25.

business enterprises, associations and groups with or without legal personality.[43]

The **data controller** is the party who is competent to decide about the contents and use of personal data, even where an agent collects or processes the data on the controller's behalf.[44] The controller is also the party who is accountable for compliance with the basic principles stated in the OECD Guidelines.[45]

The OECD Guidelines do not distinguish between the processing of data in the **private or public sectors**, or between **manual** and **automatic** processing, as long as the processing poses a danger to privacy and individual liberties.[46] There is therefore no intention to include the collection of data of an

---

43 Some member countries were of the opinion that business enterprises, associations and other groups of persons should also be protected under the OECD Guidelines. Arguments in favour of this view were the following:
- It is difficult to define clearly the dividing line between personal and non-personal data (eg, data relating to a small company may also concern its owner or owners and provide personal information of a sensitive nature).
- People belonging to a particular group (eg mentally disabled persons, immigrants, ethnic minorities) may need additional protection against the dissemination of information relating to that group.

However, not enough consensus could be reached on this issue, and the OECD Guidelines were therefore only made applicable to natural persons as data subjects. Arguments in favour of this approach were:
- The notions of individual integrity and privacy are in many respects particular and should not be treated in the same way as the integrity of a group of persons, or corporate security and confidentiality.
- The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another.

(See OECD Guidelines Explanatory Memorandum 24.)

44 OECD Guidelines par 1(a). The data controller may be a juristic or natural person, public authority, agency or any other body. However, the definition excludes four categories which may be involved in the processing of data, namely:
(a) licensing authorities and similar bodies which authorise the processing of data but are not entitled to decide what activities should be carried out and for what purposes
(b) data processing service bureaus which carry out data processing on behalf of others
(c) telecommunications authorities and similar bodies which act as mere conduits
(d) "dependent users" who may have access to data, but are not authorised to decide which data should be stored, who should be able to use them, etc

(See OECD Guidelines Explanatory Memorandum 26.)

45 OECD Guidelines Explanatory Memorandum 26.

46 OECD Guidelines par 2. On the concept "privacy and individual liberties" see fn 34.

innocent nature (for example, personal notebooks).[47]

The Group of Experts who developed the OECD Guidelines devoted special attention to the issue of whether or not the OECD Guidelines should be restricted to the **automatic** or computer-assisted **processing** of data. They identified the following reasons why such a restriction may seem to be desirable: the particular dangers to individual privacy raised by automation and computerised data banks; an increasing dominance of automatic data processing methods, especially in transborder data flows; and the particular framework of information, computer and communications policies within which the Group of Experts had set out to fulfil its mandate.

However, the Group of Experts concluded that limiting the OECD Guidelines to the automatic processing of personal data would have considerable drawbacks. First, it is difficult to draw a clearly defined distinction between the automatic and the nonautomatic handling of data, since there are "mixed" data processing systems and there are stages in the processing of data which may or may not lead to automatic treatment. Second, ongoing technological developments add to the difficulties (for example semi-automated methods based on the use of microfilm, or microcomputers which may increasingly be used for private purposes that are both harmless and impossible to control). Third, concentrating exclusively on computers in the OECD Guidelines might give rise to inconsistency and lacunae, and create opportunities for record-keepers to circumvent rules made in order to implement the OECD Guidelines by using nonautomatic means for purposes which may be offensive.[48]

The OECD Guidelines permit member countries to **limit the scope** of the measures they introduce in order to implement the OECD Guidelines. Member countries are permitted to apply the OECD Guidelines only to the automatic processing of data, to exclude personal data which obviously do not contain any risk to privacy and individual liberties, or to apply different protective measures to different

47 OECD Guidelines Explanatory Memorandum 27.

48 OECD Guidelines Explanatory Memorandum 24–25.

categories of personal data.[49]

The OECD Guidelines also recognise the fact that member countries may wish to **exclude the application** of the principles of the OECD Guidelines because of national sovereignty, national security or public policy.[50] In this regard the OECD Guidelines recommend that two general criteria ought to guide national policies: (1) These exceptions should be as few as possible and (2) they should be made known to the public.[51]

2.2.5 Basic principles of data protection

The core of the OECD Guidelines consists of the principles set out in part 2. Member countries are recommended to adhere to these principles with a view to attaining the objectives of the OECD Guidelines.[52]

The eight principles set out in the OECD Guidelines should be treated as a whole, because there is some degree of duplication and the distinctions between different activities and stages involved in the processing of data which are assumed in the principles are somewhat artificial.[53]

---

49 OECD Guidelines par 3(a)–(c).

50 OECD Guidelines par 4.

51 OECD Guidelines par 4(a)–(b). In the Explanatory Memorandum (28) it is indicated that par 4 allows for different ways of implementing the OECD Guidelines because countries are at different stages of development with regard to strategies for rules and institutions to protect privacy, and will probably proceed at different rates and apply different strategies, eg the regulation of certain types of data or activities as compared to regulation of a general nature ("omnibus approach").

The Group of Experts who compiled the OECD Guidelines foresaw that countries might apply the OECD Guidelines differently to different kinds of personal data. Examples of such areas are the balancing of competing interests such as the confidentiality of medical records versus the individual's right to inspect data relating to him or her, or in the treatment of credit reporting, criminal investigations, banking or statistical records (OECD Guidelines Explanatory Memorandum 28).

52 See par 157.

53 OECD Guidelines Explanatory Memorandum 28–29.

2.2.5.1 Principle of limitation of collection

This principle states that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.[54]

Two issues are addressed by this principle: (a) there should be limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and (b) certain requirements should be met as regards the methods employed to collect data.

a Limitation of collection of sensitive data

The Group of Experts was confronted by two opposing views as regards the enumeration of sensitive data. One view, which was supported by European legislators, was that it is both possible and desirable to enumerate types of data which are intrinsically sensitive, with the result that the collection of these types of data should be prohibited or at least restricted. Examples of such sensitive data are data that relate to race, religious beliefs and criminal records. The other view, support for which may be found in the privacy legislation of the USA, was that no data were intrinsically sensitive or private, but become so as a result of their context and use. In the end the Group of Experts found it impossible to define any set of data which were universally regarded as sensitive, and consequently only formulated a general criterion that there should be limits to the collection of personal data.[55]

---

54 OECD Guidelines par 7.

55 OECD Guidelines Explanatory Memorandum 29. The nature of the limits to the collection of data is not spelled out, but in the Explanatory Memorandum to the OECD Guidelines it is envisaged that the limits relate to:

- data quality aspects (ie that it should be possible to derive information of sufficiently high quality from the data collected, that data should be collected in a proper information framework, etc)
- limits associated with the purpose of the processing of data (ie that only certain categories of data ought to be collected, and possibly that data collection should be restricted to the minimum necessary to fulfil the specified purpose)

(continued...)

b Requirements as regards methods employed to collect data

The second part of the principle of limitation of collection is directed against practises such as the use of hidden data registration devices, or the deception of data subjects to make them supply information.[56] The Group of Experts was of the opinion that the knowledge or consent of the data subject is essential as a rule. For practical or policy reasons consent cannot always be required, but as far as possible knowledge should be the minimum requirement. However, there may also be situations where knowledge on the part of the data subject may not be appropriate, for example in criminal investigations.[57]

2.2.5.2 Data quality principle

In terms of this principle personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.[58]

The requirement that the data should be relevant to the purpose for which they are to be used means that the data should be related to that purpose.[59] The requirements of accuracy, completeness and up-to-dateness[60] are all-important aspects of data quality, and these requirements should also be linked to the

55(...continued)
- "earmarking" of specially sensitive data according to traditions and attitudes in each member country
- limits to data collection activities of certain data controllers
- civil rights concerns

56 OECD Guidelines Explanatory Memorandum 29.

57 OECD Guidelines Explanatory Memorandum 29. This principle does not exclude the possibility that a data subject may be represented by another party, eg where the data subject is a minor or a mentally disabled person (OECD Guidelines Explanatory Memorandum 29).

58 OECD Guidelines par 8.

59 Data concerning opinions or evaluative data may, eg, easily be misleading if they are used for purposes to which they bear no relation (OECD Guidelines Explanatory Memorandum 30).

The principle of relevancy as expressed in the OECD Guidelines means that all data that are included should be relevant. However, it can be argued that the principle should rather be that **all** relevant data should be included. If all relevant material is not included, the individual could just as easily be prejudiced as when irrelevant material is included (see also Bing 1984 *Michigan Yb Int Legal S* 271, 276).

60 This term is used in the OECD Guidelines Explanatory Memorandum 30. "Up-to-date" is also referred to as (continued...)

purpose to be served by the data.[61] A "purpose test" should be applied, where the issue is whether or not harm can be caused to data subjects because of lack of accuracy, completeness and updating.[62]

2.2.5.3 Purpose specification principle

This principle is closely related to the previous one (data quality principle) and to the next one (use limitation principle). The purpose specification principle requires that the purpose for which personal data are being collected should be specified not later than at the time of data collection.[63] The subsequent use of such data should be limited to the fulfilment of that purpose, or another purpose that is compatible with it, and should be specified whenever there is a change of purpose.[64] Although the principle allows for changes in the purpose, such changes should not be introduced arbitrarily. The principle also requires that when data no longer serve the purpose for which they were originally collected, they should be erased or given in anonymous form.[65]

60(...continued)
"timely" in some national legislation (see eg UK Data Protection Act of 1984).

61 According to the Group of Experts these requirements are not meant to be more far-reaching than is necessary for the purposes for which the data are used. Historical data may often have to be collected or retained for long periods, eg for social research (involving longitudinal studies of developments in society), historical research, or for archival purposes (OECD Guidelines Explanatory Memorandum 30).

62 OECD Guidelines Explanatory Memorandum 30.

63 Bing 1984 *Michigan Yb Int Legal S* 271, 277 points to a shortcoming in the OECD Guidelines, viz that they do not require that the purpose should be a legitimate one. All that is required is that the data should relate to the stated purpose, which implies that any stated purpose will do. He gives as an example the collection of data on members of extreme political parties by a bank, in order to distribute this information to its clients. This should be illegal, since the purpose is not related to banking (see Bing 1984 *Michigan Yb Int Legal S* 271, 301 fn 32).

64 OECD Guidelines par 9. Such specification of purpose can be made in alternative or complementary ways, eg by public declarations, information to data subjects, legislation, administrative decrees, and licenses provided by supervisory bodies (OECD Guidelines Explanatory Memorandum 30).

65 OECD Guidelines Explanatory Memorandum 30.

2.2.5.4 Use limitation principle

According to the use limitation principle, personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle, except with the consent of the data subject or by the authority of law.[66]

This principle deals with uses (for example disclosure) of data that deviate from the original purpose, and thus regulates the dissemination of the data.[67] The general rule is that subsequent use made of data should be compatible with the original stated purpose. However, this principle envisages that with the consent of a data subject, or by the authority of law,[68] an exception can be made to this rule.

2.2.5.5 Security safeguards principle

This principle states that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.[69]

This principle imposes an obligation on the data controller to ensure that reasonable security measures are in place to protect the privacy of the personal data. Such security measures may be physical, organisational or informational.[70] "Loss" of data includes accidental erasure of data, destruction of data because the storage media have been destroyed, and theft of the storage media; "modified" also covers

66 OECD Guidelines par 10.

67 Bing 1984 *Michigan Yb Int Legal S* 271, 278.

68 It may eg be provided by law that data which have been collected for purposes of administrative decision making may be made available for research, statistical analysis or social planning (OECD Guidelines Explanatory Memorandum 30).

69 OECD Guidelines par 11.

70 Physical measures include the use of locked doors and identification cards; organisational measures would eg be the use of access codes that are given to certain persons only; and informational measures would include enciphering or monitoring of unusual activities (OECD Guidelines Explanatory Memorandum 31).

unauthorised input of data and "use" includes unauthorised copying.[71]

2.2.5.6 Openness principle

This principle requires that there should be a general policy of openness about developments, practices and policies in respect of personal data. Means should be readily available to establish the existence and nature of personal data, the main purposes for which they are used, as well as the identity and usual residence of the data controller.[72]

The openness principle is a prerequisite for the next principle (individual participation), because if individuals are to be able to participate it should first be possible for them to learn about information kept on them.[73] This principle can be complied with in any one of several ways, examples of which are:

- regular information from data controllers to data subjects
- publication in official registers of descriptions of activities concerned with the processing of personal data
- registration by data controllers with public bodies[74]

The requirement that the means should be "readily available" implies that the individual should be able to obtain the information without unreasonable effort as to time, money, or travelling.[75]

2.2.5.7 Individual participation principle

In terms of this principle, individuals should have the right to obtain from a data controller, or by other

71 OECD Guidelines Explanatory Memorandum 31.

72 OECD Guidelines par 12.

73 The openness principle has been dubbed the "magna carta of the computer age" (Bing 1984 *Michigan Yb Int Legal S* 271, 280).

74 OECD Guidelines Explanatory Memorandum 31.

75 OECD Guidelines Explanatory Memorandum 31.

means, confirmation as to whether or not the data controller has data relating to them, and to have such data communicated to them within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner and in a form that is readily intelligible to them. Furthermore, individuals should have the right to be given reasons if a request is denied, and to be able to challenge such denial. Individuals should also have the right to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended.[76]

The Group of Experts was of the opinion that the individual participation principle was the most important privacy protection safeguard, and consequently spelled out this principle in much greater detail than the others.[77]

a Right to access

This right should be simple to exercise and should not involve legal processes. Intermediate access may be used where appropriate, for example in the medical field where a medical doctor may act as the intermediary.[78] Supervisory institutions, such as data inspection authorities, could serve a similar function.

The requirement that the access should be granted **within a reasonable period of time** may be complied with in different ways. For example, if a data controller supplies information on a regular basis, such controller may be exempted from responding immediately to an individual request. The length of time taken to respond is usually counted from receipt of the request, and what is a reasonable length of time may vary according to the circumstances.

The requirement that the data should be communicated **in a reasonable manner** means that, among others, problems resulting from geographical distance should be given proper attention. Although it is permissible to specify the periods within which requests should be met, such periods should be

76 OECD Guidelines par 13.

77 OECD Guidelines Explanatory Memorandum 31–32.

78 This idea is also reflected in the EU Directive (see fn 319).

reasonable. The extent to which data subjects should be able to obtain copies of the data relating to them should be determined by each individual member country.

b Right to reasons

The right to reasons is used in the narrow sense that reasons should be given for refusal of requests. This narrow usage may be broadened by individual member countries to include the right to reasons for any adverse decision made.

c Right to challenge

The right to challenge is broad and includes challenges to data controllers, as well as subsequent challenges in courts or to administrative bodies, professional or other institutions, according to domestic rules of procedure. This does not mean that data subjects may decide which remedy they want to use – the procedures may be prescribed by domestic law.

The Guidelines state that a data subject may, if his or her challenge is successful, have the data erased, rectified, completed or amended.[79] According to Bing, completion or amendment of data would be the appropriate remedy where for practical reasons data cannot be erased or rectified.[80]

2.2.5.8 Accountability principle

This principle states that a data controller should be accountable for complying with measures which

79 OECD Guidelines par 13.

80 Bing 1984 *Michigan Yb Int Legal S* 271, 281. Bing gives the example of a newspaper that publishes invalid information from a data file. Since the data subject cannot ask for a rectification or erasure of such news item after publication, an explanation as a correction to the item should serve as an "amendment" or "completion".

give effect to the principles stated above.[81]

Since the data processing activities are carried out for the benefit of the data controllers, the controllers should be accountable under domestic law for complying with privacy protection rules and should not be relieved of this accountability merely because service bureaus carry out the data processing activities on their behalf.[82] However, member countries may decide to extend accountability to service bureaus or dependent users.[83] Accountability under this principle refers to accountability supported by legal sanctions, or imposed by codes of conduct.[84]

2.2.6 National implementation – enforcement of principles

The manner in which countries should implement the principles of the OECD Guidelines is not precisely prescribed. However, a general framework is given indicating in broad terms what kind of national machinery is envisaged.[85]

The OECD Guidelines provide that legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data should be established. Member countries have a particular responsibility to adopt domestic legislation appropriate to their law,[86] encourage and support self-regulation, whether in the form of codes of conduct or otherwise;[87] provide

81 OECD Guidelines par 14.

82 OECD Guidelines Explanatory Memorandum 32.

83 Breaches of confidentiality may eg be sanctioned in the case of dependent users as well (OECD Guidelines Explanatory Memorandum 32).

84 OECD Guidelines Explanatory Memorandum 32.

85 OECD Guidelines par 19.

86 OECD Guidelines par 19(a). Legislation is not the only means by which the OECD Guidelines can be enforced, however.

87 OECD Guidelines par 19(b).

for reasonable means for individuals to exercise their rights;[88] provide for adequate sanctions and remedies in case of failure to comply with measures which implement the principles of the Guidelines;[89] and ensure that there is no unfair discrimination against data subjects.[90]

2.2.7 Transfer of data to third countries

As stated previously, the OECD Guidelines have two goals, namely the setting of standards at the national level for the protection of privacy in personal records, and the reconciliation of this ideal with the ideal of the free flow of information across national boundaries.[91] The second issue is dealt with in paragraphs 15 to18 of the OECD Guidelines.

The principles embodied in these paragraphs are all interrelated. Paragraph 15[92] emphasises the principle that member countries should respect each other's interest in protecting personal data, and the privacy and individual liberties of their national residents. It is directed against policies which facilitate attempts to circumvent or violate the protective legislation of other member countries, and it encourages member countries to consider the need to adapt rules and practices for the processing of data to the particular circumstances which may arise when foreign data and data on non-nationals are involved.[93]

---

88 OECD Guidelines par 19(c). A broad interpretation should be given to par 19(c), and it should be interpreted to include means such as advice from data controllers and the provision of assistance, including legal aid (OECD Guidelines Explanatory Memorandum 34–35).

89 OECD Guidelines par 19(d). Par 19(d) permits different approaches to the issue of control mechanisms, eg the setting up of special supervisory bodies and reliance on existing control facilities (such as the courts or public authorities) (OECD Guidelines Explanatory Memorandum 35).

90 OECD Guidelines par 19(e). Par 19(e) is directed against discrimination based on race, domicile, sex, creed or trade union affiliation, but allows "benign" discrimination to support disadvantaged groups (OECD Guidelines Explanatory Memorandum 35).

91 Also see par 2.2.3 and fn 6 and accompanying text.

92 OECD Guidelines par 15: "Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data."

93 OECD Guidelines Explanatory Memorandum 33.

Paragraph 16 deals with security issues at the international level. It requires member countries to take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country are uninterrupted and secure, in other words, protected against unauthorised access and loss of data.[94]

Paragraph 17 provides for three exceptions to the general rule that a member country should refrain from obstructing the transborder flow of data between itself and another member country in the following circumstances:

- ❒ if the receiving member country is not substantially observing the OECD Guidelines, in other words if it does not have acceptable data protection rules[95]

- ❒ if the receiving member country is only acting as a transit country for another country which has not implemented the OECD Guidelines

- ❒ if the member country has imposed restrictions on personal data of a special nature, and the receiving member country does not have similar provisions[96]

Paragraph 18[97] attempts to ensure that privacy protection interests are balanced against considerations of free transborder flows of personal data. It is aimed at preventing the creation of barriers that do not serve to protect privacy and individual liberties, but other interests that are not openly announced, for example economic protectionism.[98]

---

94 OECD Guidelines Explanatory Memorandum 33.

95 This is the principle of "equivalence" (see fn 7).

96 The third exception also involves the principle of "equivalence" (see fn 7).

97 OECD Guidelines par 18: "Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."

98 OECD Guidelines Explanatory Memorandum 34. The USA delegation to the OECD meeting was concerned (continued...)

2.2.8 International cooperation

The OECD Guidelines also make provision for cooperation between the member countries. They provide that any member country should on request provide other member countries with information about rules, regulations and decisions taken by that member country in order to implement the OECD Guidelines.[99] The Guidelines instruct member countries to ensure that transborder flows of personal data are not hampered by unnecessarily complex and disparate frameworks of procedures and compliance requirements.[100]

The OECD Guidelines also provide that member countries should establish procedures to facilitate information exchange related to the Guidelines, and stipulate that there should be mutual assistance between countries with the procedural and investigative matters involved.[101] This provision was based on the assumption that the OECD Guidelines would form the basis for continued future cooperation,[102] and the practical significance of this provision was expected to increase as the data networks, and the problems associated with them, grew.[103]

2.2.9 Conflict of laws and jurisdiction

98(...continued)
that data protection measures could be used for economic protectionism (Lloyd *Information technology law* 48). Also see fn 3.

99 This problem arises because of the complexity of privacy protection regulation and data policies in general – there are often several levels of protection and important rules are often left open for interpretation by lower-level decision making bodies (OECD Guidelines Explanatory Memorandum 35).

100 OECD Guidelines par 20. This problem is proportional to the number of domestic laws which affect transborder flows of personal data. There is a need for co-ordinating special provisions on transborder flows in domestic laws, which include arrangements that relate to compliance control and licenses to operate data processing systems (OECD Guidelines Explanatory Memorandum 35).

101 OECD Guidelines par 21.

102 The Council recommended to the member countries that they should agree as soon as possible on specific procedures of consultation and cooperation for the application of the OECD Guidelines (par 4 of Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data).

103 OECD Guidelines Explanatory Memorandum 35.

When data are transferred between several member countries, the issue of conflict of laws and a choice of jurisdiction may arise. In view of the rapid changes in technology, the OECD Guidelines do not attempt to offer any detailed solution in this regard; instead it is left to the member countries to work towards a solution.[104]

2.3 Conclusion

The OECD Guidelines contain the basic principles of data protection and they endeavour to balance the protection of privacy against the principle of the free flow of data. The member countries of the OECD include the most important countries in the information communications arena, namely the USA and most European countries. Consequently, the Guidelines were a very important document at the time of adoption. However, because they were not legally binding, and because they allowed for considerable variation in the way they were implemented by member states,[105] they were not sufficient to "ensure the

104 OECD Guidelines par 22 provides: "Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data." The Group of Experts made the following comments on the issue of choice of law (OECD Guidelines Explanatory Memorandum 36):

> As regards the question of choice of law, one way of approaching these problems is to identify one or more connecting factors which, at best, indicate **one** applicable law. This is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied. For one thing, the appropriateness of such a solution seems to depend upon the existence of both similar legal concepts and rule structures, and binding commitments of nations to observe certain standards of personal data protection. In the absence of these conditions, an attempt could be made to formulate more flexible principles which involve a search for a "proper law" and are linked to the purpose of ensuring effective protection of privacy and individual liberties. Thus, in a situation where several laws may be applicable, it has been suggested that one solution could be to give preference to the domestic law offering the best protection of personal data. On the other hand, it may be argued that solutions of this kind leave too much uncertainty, not least from the point of view of the data controllers who may wish to know, where necessary in advance, by which national systems of rules an international data processing system will be governed.

105 Eg, the USA did not enact legislation in the private sector to implement the OECD Guidelines, but encouraged the private sector to voluntarily comply with their provisions.

functioning of the global market".[106]

2.4 OECD initiatives following OECD Guidelines

Since the adoption of the Guidelines, an *ad hoc* meeting of Experts on the protection of privacy has been convened every three years to enable national delegations to present developments in the area and to discuss topical issues.[107] At the request of the ICCP Committee,[108] the OECD has held annual meetings since 1990 on a range of data protection issues.[109] In 1988, the OECD's interest in data protection was also illustrated by the creation of a Commission for Computerized Information and Privacy whose duties included the regulation of the creation and use of personal data files by the OECD Secretariat.[110] Other initiatives by the OECD include a Declaration on Transborder Data Flows adopted in 1985 by the Ministers of the OECD member countries, the Guidelines for the Security of Information Systems adopted in 1992,[111] and the Guidelines for Cryptography Policy", issued in 1997.[112] In 2000 the OECD posted a Privacy Policy Statement Generator on its Web site. This enables businesses and other organisations to create a privacy policy statement for online use. The objective is to raise public awareness of the importance of privacy online and to contribute to building consumer confidence in online transactions. It saves companies time and effort in developing privacy policies, and enables them to post statements that are consistent with globally recognised privacy rights.[113]

---

106 Blume 1992 *Computer/L J* 399, 405.

107 Franklin *Business guide* 558.

108 See fn 19.

109 Franklin *Business guide* 558.

110 Madsen *Personal data protection* 25.

111 Franklin *Business guide* 559.

112 One of the stated purposes of these Guidelines is to promote the use of cryptography to help ensure the security of data and to protect privacy in national and global information and communications infrastructures, networks and systems. This document can be found on the OECD webpage (http://www.oecd.org).

113 See 2000 *Computer Law & Sec Rep* 70.

3 COUNCIL OF EUROPE CONVENTION ON DATA PROTECTION

3.1 Introduction

The Council of Europe is an intergovernmental institution, consisting of the heads of state or government, that meets twice a year and undertakes certain activities which remain outside the legal authority of the EU.[114] It serves as a forum for a broad range of European countries.[115] The history of the Council of Europe Convention on data protection,[116] which was adopted on 28 January 1981, goes back to 1968, when the Parliamentary Assembly of the Council of Europe requested the Committee of Ministers[117] to consider whether the European Convention on Human Rights[118] and the domestic law of the member

114 The Council of Europe was established in May 1949 to enable the governments of (at that stage) twenty-six European States to cooperate "to achieve a greater unity between its members for the purpose of safeguarding and realising ideals and principles which are their common heritage and facilitating their economic and social progress" (a 1 of the Statute of the Council – quoted in Ausems "Council of Europe" 537). This purpose is achieved by the conclusion of agreements and conventions and the adoption of common policies in all spheres of public life except national defence (Hondius *Emerging data protection* 63; Beling 1983 *Boston College Int & Comp L R* 591, 593 fn 23. See also Archer & Butler *European Community* 28; Hill *European Community* 7).

115 By 2003 the Council comprised 44 European countries, including Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, San Marino, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, and the United Kingdom, as well as a handful of non-European countries.

116 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data No 108/1981. Hereafter cited as Convention 108/1981 and referred to as "the Convention". Note that the Convention is sometimes referred to by its number, ie Convention 108 (see eg Ausems "Council of Europe" 537). Also see fn 4.

117 The Council is governed by an intergovernmental Committee of Ministers with powers of decision and recommendation (consisting of the foreign ministers of the governments of the member countries) which is advised by the Parliamentary Assembly, an inter parliamentary deliberative body. The Council is based in Strasbourg, France. The Convention under discussion is therefore sometimes referred to as the "Convention of Strasbourg" (see eg Hofman *Vertrouwelijke communicatie* 95).

118 The Council of Europe is in charge of the European Convention on Human Rights (Blume 1992 *Computer/L J* 399, 405), which provides, *inter alia*, that everyone has a right to privacy. The right to privacy is laid down in article 8:

> 1 Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country,

(continued...)

states offered adequate protection to the right of personal privacy *vis-à-vis* modern science and technology.[119] In 1970 the Committee of Experts on Human Rights, to whom the request was passed on, reported that the protection offered under present national legislation was inadequate. Two issues were highlighted: (1) the possibility of the infringement of individuals' rights through the use of computers in the private sector,[120] and (2) the conflict that existed between the individual's claim to a greater measure of control over personal information[121] and the individual's claim to be allowed access to information under the European Convention of Human Rights.[122]

As a result the Committee of Ministers adopted two resolutions[123] to establish minimum standards of privacy protection with respect to information in "electronic banks". The Committee of Experts stressed that after the member states have enacted national legislation based on these resolutions, the next step

118(...continued)
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.
The European Convention on Human Rights was signed in Rome on 4 November 1950, and ratified by all member states of the European Communities (Nugter *Transborder flow of personal data* 286).

119 Convention 108/1981 Explanatory Report par 4; Lloyd *Information technology law* 45; Walden "Data protection" 446; Campbell *Data transmission and privacy* 140.

120 The European Convention on Human Rights was largely based on the premise that the individual's rights might be infringed by the actions of public authorities (Lloyd *Information technology law* 45).

121 Ie data protection.

122 Ie freedom of information. A 10 of the European Convention on Human Rights provides: "Everyone has the right to freedom of expression. This shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."
In 1986 the Council of Europe returned to the issue of data protection and freedom of information. The Parliamentary Assembly approved a Recommendation on Data Protection and Freedom of Information. This restated the potential for conflict between the two concepts. However, Lloyd *Information technology law* 45 points out that it is also true that both concepts seek to improve the position of individuals against those organisations which hold information that is relevant to their lives, and therefore the concepts are not inherently opposed.

123 Resolution 73(22) on the Protection of the Privacy of Individuals Vis-à-vis Electronic Data Banks in the Private Sector in 1973 and Resolution 74(29) on the Protection of the Privacy of Individuals Vis-à-vis Electronic Data Banks in the Public Sector in 1974. For a discussion of these resolutions, see Campbell *Data transmission and privacy* 140; Bing 1984 *Michigan Yb Int Legal S* 271, 272; Hondius *Emerging data protection* 67–68; Nugter *Transborder flow of personal data* 25.

should be the reinforcement of these rules by means of a binding international agreement.[124] Within five years after the resolutions had been adopted, seven Council of Europe member states passed data protection legislation.[125] The Committee of Experts was instructed to prepare a text for a convention on data protection.[126] The text of the Convention for the Protection of Individuals with regard to Automatic Processing of Data[127] was approved by the Committee of Ministers on 17 December 1980, was made available for signature on 28 January 1981 and came into force in 1985, having been ratified by five countries,[128] as required.[129] By 1994, the Convention had been signed by twenty-one countries,[130] and ratified by sixteen countries, including the UK and the Netherlands.[131]

124 Convention 108/1981 Explanatory Report par 12.

125 Austria, Denmark, France, Germany, Luxembourg, Norway and Sweden (see Campbell *Data transmission and privacy* 140).

126 The committee was instructed to do so in close collaboration with the OECD, including the non-European member countries of that organisation. Close contact was kept between these two organisations, as well as the Commission of the European Communities and the European Parliament (see fn 204). The OECD, and four of its non-European member countries (Australia, Canada, Japan and the USA) were represented by an observer on the Council of Europe's committee. Observers from Finland, the Hague Conference on Private International Law and the European Communities also took part in the work (Convention 108/1981 Explanatory Report par 14–15). Consequently, the Convention and the OECD guidelines are similar in many respects (see also Hondius 1983 *Neth Int L R* 103, 113).

127 See fn 4.

128 Sweden (1982), France (1983), Norway (1984), Spain (1984) and Germany (1985) (Nov/Dec 1994 *TDR* 33).

129 Convention 108/1981 a 22(2).

130 Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Slovenia, Spain, Sweden, Turkey, and the United Kingdom (Nov/Dec 1994 *TDR* 33). The Convention is an open Convention, ie it is open to signature by states which are not members of the Council of Europe (Jay 1989 *Computer L & Prac* 134, 135).

131 Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Luxembourg, the Netherlands, Norway, Portugal, Slovenia, Spain, Sweden and the UK. By 1998, 20 parties had contracted to the Convention (Data Protection Working Party *Second annual report* 31).

3.2 Provisions of Convention[132]

3.2.1 Overview of structure of Convention

The Convention consists of three main parts: substantive law provisions in the form of basic principles, special rules on transborder data flows, and mechanisms for mutual assistance and consultation between the parties.[133]

3.2.2 Purpose of Convention

The purpose of the Convention is to secure in the territory of each party[134] for all individuals, whatever their nationality or residence, respect for their rights and fundamental freedoms, in particular their right to privacy, with regard to automatic processing of personal data relating to them.[135] In other words, the Convention aims to set standards for data protection at the national level. However, it also has a further purpose, namely to ensure the free flow of data at the international level. Consequently, the Convention contains provisions not only on data protection, but also on transborder data flows. Its aim is thus to reconcile the two competing requirements of free flow of information[136] and data protection.[137]

---

132 For a discussion of the Convention, see Evans 1981 *Am J Comp L* 571–582; 1981 *J World Trade L* 150, 154 *et seq*; Williams 1982 *Annals of Air & Space L* 447, 456–467; Beling 1983 *Boston College Int & Comp L R* 591, 603–618; Hondius 1983 *Neth Int L R* 103, 112–125; Bing 1984 *Michigan Yb Int Legal S* 271–303; Early 1986 *Computer L & Prac* 68–69; Frosini 1987 *Computer L & Prac* 84–90; Campbell *Data transmission and privacy* 140–147.

133 Convention 108/1981 Explanatory Report par 18.

134 Non-European countries may also be parties to the Convention (Convention 108/1981 a 23 and Explanatory Report par 24).

135 Convention 108/1981 a 1.

136 The free flow of information is embodied in a 10 of the European Convention on Human Rights. See fn 122.

137 Convention 108/1981 Explanatory Report par 21. The commentary on the Convention stresses that "no other motives" than to "maintain a just balance between the different rights and interests of individuals" could justify the data protection rules of the Convention. "It is also underlined that the convention should not be interpreted as a means to erect non-tariff barriers to international trade or to restrain the exchange of scientific and cultural information" (Explanatory Report par 25). Also see Williams 1982 *Annals of Air & Space L* 447, 459.

3.2.3 Scope of Convention

The parties to the Convention must apply its principles to **automated data files**, and to **automatic processing** of **personal data** (by a **controller**) in the **public and private sectors**.[138]

Automated data files are any set of data undergoing automatic processing,[139] and **automatic processing** includes the following operations, if carried out in whole or in part by automated means: storage of data, carrying out of logical and / or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.[140]

Personal data are information relating to an identified or identifiable individual, also called the **data subject**.[141] A **controller** is the natural or juristic person, public authority, agency or any other body that is competent in terms of the applicable national law to decide what the purpose of the automated data file should be, which categories of personal data should be stored and which operations should be applied to such data.[142]

Parties may, however, **extend the scope** of the Convention to information relating to groups of persons, associations, foundations, companies, etcetera, whether or not they possess legal personality,[143] as well

138 Convention 108/1981 a 3(1).

139 Convention 108/1981 a 2(b). The term "data file" replaces the term "data bank" previously used in Resolutions 7322 and 74(29) (see fn 123), because "data bank" was subsequently used in the specialised sense of a "pool of data accessible to several users" (Convention 108/1981 Explanatory Report par 30). See Hondius 1983 *Neth Int L R* 103, 114–115 for a discussion of the problems drafters of international documents have in a field where there are rapid technological advances.

140 Convention 108/1981 a 2(c).

141 It is stressed (Convention 108/1981 Explanatory Report par 29) that the notion of a "data subject" expresses the idea that a person has a subjective right with regard to information about himself, even where this is gathered by others.

142 Convention 108/1981 a 2(d).

143 Convention 108/1981 a 3(2)(b). This extension is effected by giving notice to the Secretary General of the Council of Europe at the time of signature or any later time.

as to personal data files which are not processed automatically.[144] Parties may also exclude certain categories of automated personal data files.[145] A list of the categories that are excluded must be deposited.[146]

3.2.4 Basic principles of data protection

The Convention is based on a number of basic principles of data protection upon which each member country is expected to draft appropriate legislation.[147] Each contracting state should give effect to these principles in its domestic legislation, since the Convention is not self-executing.[148] It is left to the parties to decide exactly how they want to give effect to the principles.[149] These principles guarantee certain minimum protection[150] with regard to the automatic processing of personal data to data subjects in all countries, and should result in harmonisation of the laws of the parties, which will ensure that the principle

144 Convention 108/1981 a 3(2)(c). France has made a declaration extending the scope of its data protection legislation to include manual files (Campbell *Data transmission and privacy* 143).

145 Declarations excluding categories of data files have been made by Norway, the United Kingdom, Luxembourg and Ireland (see Campbell *Data transmission and privacy* 142).

146 Convention 108/1981 a 3(2)(a). However, this may not include categories of automated data files subject under its domestic law to data protection provisions. A party to the Convention which has excluded certain categories of automated personal data files may not claim the application of the Convention to such categories by another party which has not excluded them. Likewise, a party which has not made any of the extensions provided for may not claim the application of the Convention on these points with respect to a party which has made such extensions (Convention 108/1981 a 3(4) and (5)).

147 Convention 108/1981 a 4(1); Walden "Data protection" 446. Chalton et al *Encyclopedia of data protection* par 1–038 describes the importance of these principles as follows:

> These are the eight commandments which the Council of Europe brought down from the mountain and which the European Convention requires to be implemented within the domestic laws of each party State.

148 In other words, the Convention only forms part of the law of a member state if that state formally adopts it (Convention 108/1981 Explanatory Report par 38). This also means that individuals cannot invoke the Convention before their national court (Nugter *Transborder flow of personal data* 25–26).

149 The measures can take different forms, such as laws, regulations, administrative guidelines etc (Convention 108/1981 Explanatory Report par 39). Voluntary measures, such as codes of conduct, are not sufficient (Campbell *Data transmission and privacy* 143).

150 A contracting state may grant data subjects a wider measure of protection than that stipulated in the Convention (Convention 108/1981 a 11). In other words, domestic standards may exceed these basic standards (Schwartz 1995 *Iowa L R* 471, 477).

of free flow of information will not be jeopardised.[151] Member states may grant data subjects a wider measure of protection than that stipulated in the Convention.[152]

3.2.4.1 Principles regarding quality of data

It is provided that personal data undergoing automatic processing should be obtained and processed[153] fairly and lawfully, stored for specified and legitimate purposes and not used in a way incompatible with those purposes; be adequate, relevant and not excessive in relation to the purposes for which they are stored; be accurate and, where necessary, kept up to date; and be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[154]

3.2.4.2 Principles regarding special categories of data / sensitive data

It is provided that personal data revealing racial origin, political opinions or religious or other beliefs,[155] as well as personal data concerning health[156] or sexual life, or relating to criminal convictions, may not be processed automatically unless domestic law provides appropriate[157] safeguards.[158] The list is not

151 Convention 108/1981 Explanatory Report par 20 and 21.

152 Convention 108/1981 a 11.

153 The Convention makes a distinction between "obtaining" and "processing" of information. This distinction disappears in the EU Directive, discussed subsequently (see fn 238 and accompanying text).

154 Convention 108/1981 a 5.

155 Including activities resulting from such opinions or beliefs (Convention 108/1981 Explanatory Report par 44).

156 This includes information concerning the past, present and future physical or mental health of an individual. It may refer to a person who is sick, healthy or deceased. This category of data also covers data relating to alcohol abuse or the taking of drugs (Convention 108/1981 Explanatory Report par 45).

157 Evans 1981*Am J Comp L* 571, 578–579 argues that a broad term such as "appropriate" leaves the contracting parties with a "broad margin of appreciation as regards the safeguards they are to provide and thus detracts severely from the value of the article".

158 Convention 108/1981 a 6. It is felt that although the risk that data protection is harmful to persons generally

(continued...)

meant to be exhaustive, and a contracting state may include other categories in its domestic law.[159]

3.2.4.3 Principles regarding data security

The Convention requires that appropriate[160] security measures should be taken for the protection of personal data stored in automated data files, against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.[161] This implies that there should be specific security measures for every file, taking into account its degree of vulnerability, the need to restrict access to the information within the organisation, requirements concerning long-term storage, etcetera. The security measures should reflect the current state of the art of data security techniques and methods in the field of data processing.[162]

3.2.4.4 Principles regarding rights of data subject[163]

The Convention requires that any person should have the following rights:

- Be able to establish that an automated personal data file exists, what its main purposes are, and what the identity and habitual residence or principal place of business of the controller of the

158(...continued)
depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachment on individual rights and interests (Convention 108/1981 Explanatory Report par 43).

159 Convention 108/1981 Explanatory Report par 48. It is acknowledged that the degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned.

160 "Appropriate security measures" means that the measures should be adapted to the specific function of the file and the risks involved (Convention 108/1981 Explanatory Report par 57).

161 Convention 108/1981 a 7.

162 Convention 108/1981 Explanatory Report par 49.

163 The Convention does not use the term "rights" but refers to "additional safeguards" for the data subject. This is because the Convention itself does not bestow rights on data subjects, since it is not self-executing.

file are.[164]

- ❒ Be able to obtain at reasonable intervals and without excessive delay or expense, confirmation of whether personal data relating to him or her are stored in the automated data file as well as communication to him or her of such data in an intelligible form.[165]

- ❒ Be able to obtain either rectification or erasure of personal data that have been processed in a manner contrary to the provisions of domestic law, giving effect to the basic principles of the Convention.[166]

- ❒ Have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure is not complied with.[167]

3.2.4.5 Exceptions and restrictions

A contracting state may derogate from the provisions regarding the quality of data, special categories of data, and the rights of data subjects only if this is provided for in its national law, and if this constitutes a necessary measure in a democratic society in the interest of protecting either state security, public

164 Convention 108/1981 par 8(a).

165 Convention 108/1981 a 8(b). There is no provision which stipulates that the data subjects should be informed that information about them is being processed, or that their consent must be obtained before processing can take place (see eg the provisions of the EU Directive in this regard – par 4.2.4.) However, another principle requires that data should be obtained and processed fairly and lawfully (see par 3.2.4.1). It can be argued that processing can in general only take place fairly and lawfully if the data subjects have consented thereto or know about it.

166 Convention 108/1981 a 8(c).

167 Convention 108/1981 a 8(d). Convention 108/1981 a 8(d). Hondius 1983 *Neth Int L R* 103, 116–117 describes the "classic trio" of rights, namely the right to know, the right to correction and erasure and the right to a remedy in the case of refusal, as "the most important legal innovation which data protection has achieved, both in domestic law and international law."

safety, the monetary interests of the state[168] or the suppression of criminal offences,[169] or protecting the data subject or the rights and freedoms of others.[170]

3.2.5 Sanctions and remedies

The Convention provides that sanctions and remedies should exist for violations of data protection rights.[171] However, in the light of the non self-executing nature of the Convention, it is left to the contracting states to determine the nature of these sanctions and remedies, that is civil, administrative or criminal.[172]

3.2.6 National implementation: enforcement of principles

The Convention does not require of parties to it to have an independent data protection authority,[173] or any other regulatory scheme for that matter. However, as seen, it does require that sanctions and remedies should exist for violations of data protection rights.[174]

---

168 Eg, tax collection requirements and exchange control (Convention 108/1981 Explanatory Report par 57).

169 This includes the investigation as well as the prosecution of criminal offences (Convention 108/1981 Explanatory Report par 57).

170 Convention 108/1981 a 9(2). The restrictions relate to the exceptions made to the right to privacy, freedom of religion, freedom of expression and freedom of association, by the second paragraphs of articles 8, 9, 10 and 11 of the European Convention on Human Rights (Hondius 1983 *Neth Int L R* 103, 117). For a discussion of the European Convention on Human Rights, see Harris, O'Boyle & Warbrick *European Convention on Human Rights*. The Convention is silent on whether exceptions should be made to accommodate freedom of information.

171 Convention 108/1981 a 10.

172 Convention 108/1981 Explanatory Report par 60.

173 The reason for this is that the Council of Europe wanted to keep the Convention open to the widest possible number of countries, including those who leave supervision in the hands of the ordinary courts or some other authority (Hondius 1983 *Neth Int L R* 103, 119).

174 See par 3.2.5.

3.2.7 Jurisdiction, applicable law and conflict of laws[175]

The Convention contains no provisions with regard to the above, apparently because it was feared that this matter could delay its adoption.[176] It was also argued that the presence of a common core of substantive law, parts of which harmonise procedure, would help to reduce the risk of conflict of laws or legal lacunae.[177]

3.2.8 Transfer of data to third countries

As a general rule, a contracting state may not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation the transfer of personal data[178] to the territory of another contracting state,[179] unless its legislation provides a higher level of protection for the category of personal data involved than that provided for in the Convention.[180] However, if the recipient country provides an equivalent level of protection, such a barrier is not allowed.[181] In other words, the standard that is employed when deciding whether international transfer of personal data may take place is an

175 Hondius 1983 *Neth Int L R* 103, 120 identifies three basic questions that arise when data files, the controllers of those files, the data users or the data subjects are located in different countries: (a) What authority is competent? (b) What law is to be applied? (c) How could decisions in application of those laws be executed? Also see Bing *Reflections on a data protection policy* 175, who finds it surprising that the "latent problems" relating to conflict of laws, or choice of laws, have not yet realised in the field of data protection, being such an obviously international area.

176 Hondius 1983 *Neth Int L R* 103, 120.

177 Convention 108/1981 Explanatory Report par 23.

178 This provision applies to "the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed" (see Convention 108/1981 a 12(1)). Although the article refers to "personal data", it is understood that if two contracting parties have applied the principles of the Convention to juristic persons, this provision, and indeed all other provisions, will also apply to information on juristic persons (Convention 108/1981 Explanatory Report par 65).

179 Convention 108/1981 a 12(2). As pointed out (see par 3.2.2), the aim of the Convention is to reconcile the two competing requirements of free flow of information and data protection.

180 The *rationale* for this provision is that all parties that have ratified the Convention offer a certain minimum level of protection to personal data that are processed (Campbell *Data transmission and privacy* 146).

181 Convention 108/1981 a 12(3)(a).

"equivalency" standard – data protection must be "equivalent" in the recipient state, otherwise transfer of data may be prohibited.[182]

A country may restrict the transfer of personal data to another contracting state where the data will be re-exported to a third (that is, a noncontracting) state. This is to prevent such transfers resulting in the circumvention of the first country's legislation.[183] The Convention does not explicitly deal with direct transfers of personal data to non-contracting states, but it has been interpreted as requiring an equivalent standard of protection in these countries.[184]

3.2.9 Mutual assistance

The Convention makes provision for mutual assistance between the contracting states, as well as for assistance to data subjects residing abroad.

The contracting parties are required to cooperate in order to implement the Convention. For that purpose, each contracting state must designate an authority and the name of that authority must be communicated to the Council of Europe. An authority must assist another on request, for example by supplying information on its law and administrative practice in the field of data protection.[185]

The contracting states must also assist persons residing abroad to exercise the rights conferred on them by their country's data protection law.[186]

182 Schwartz 1995 *Iowa L R* 471, 472.

183 Convention 108/1981 a 12(3)(b). However, this provision may not be invoked on the mere presumption or likelihood that data will be transferred to a third country (Explanatory Report par 70).

184 Schwartz 1995 *Iowa L R* 471, 478.

185 Convention 108/1981 a 13.

186 Convention 108/1981 a 14. The Convention also contains provisions providing safeguards concerning assistance rendered by designated authorities, grounds on which a request for assistance may be refused, and a provision as regards the costs involved in the rendering of assistance (a 15, 16 and 17).

3.2.10 Consultative Committee

The Convention sets up a Consultative Committee consisting of representatives of each contracting state.[187] The purpose of the Committee is to ensure the smooth running of the Convention.[188] Its functions are to formulate proposals with a view to facilitating or improving the application of the Convention or to amend the Convention, or to advise the contracting parties.[189]

3.3 Conclusion

The Convention is not intended to displace national regulations, but by requiring signatory states to give effect to the basic principles of data protection, it seeks to create a stimulus and point of reference for domestic data protection activities.[190] However, because it does not prescribe the specific manner in which it should be implemented, there is a diversity of national interpretations of the Convention's requirements, an aspect which has led to criticism of the Convention.[191] There are differences, for example, regarding the definition of a "person". Scandinavian countries apply privacy rights to juristic persons as well as to natural persons, whereas many other countries, such as the United Kingdom and the Netherlands, do not. Differences also exist over the protection of sensitive data.[192] A major weakness of the Convention is its lack of enforceability against countries that fail to comply with the basic principles, since no enforcement machinery was created under the Convention. Any disputes have to be resolved at diplomatic level.[193]

---

187 Convention 108/1981 a 18.

188 Convention 108/1981 Explanatory Report par 86.

189 Convention 108/1981 a 19. Also see par 3.5 on the subsequent work of the Committee of Ministers' Project Group on Data Protection (known by its French acronym "CJ-PD").

190 Schwartz 1995 *Iowa L R* 471, 478.

191 Schwartz 1995 *Iowa L R* 471, 478; Raab & Bennett 1994 *Pub Adm* 95, 101.

192 Raab & Bennett 1994 *Pub Adm* 95, 101.

193 Walden "Data protection" 446.

Nevertheless, the Convention has been an important stimulus for data protection legislation in Council of Europe member countries. Before member countries could ratify the Convention, they had to adopt data protection legislation – the United Kingdom and the Netherlands, for example, adopted data protection legislation for this very reason.[194] As one commentator puts it:[195] "The force of the Council of Europe Convention, more than that of the OECD Guidelines, has continued to draw new countries into the data protection community." Before the European Union Directive on data protection was issued, the Convention formed the basis of data protection laws in many European states.[196]

3.4 Comparison between OECD Guidelines and Council of Europe Convention[197]

There are many similarities between the OECD Guidelines and the Convention. For example, the similarities in their scope of applications lie within the definitions of "personal data" and "controller" of the file, and both instruments apply to the public and the private sectors and to natural persons only. The basic principles of privacy protection and the provisions concerning transborder data flows are also similar in general, although there are some differences as regards the details.

There are also major differences between the two instruments, the most important being the difference in their legal force. Whereas the Council of Europe Convention is a contractual commitment between the signatory nations and thus legally binding for the ratifying states, the OECD Guidelines are voluntary in nature. They are not legally binding in the sense that non-compliance with their principles attracts only

194 See ch 4 par 4.2.1.1 and ch 5 par 4.2.1.

195 Bennett *Regulating privacy* 248.

196 Ausems "Council of Europe" 539.

197 See Neisingh & de Houwer *Transborder flow of personal data* 30–31; Papapavlou "Latest developments" 29 *et seq*. See also Beling 1983 *Boston College Int & Comp L R* 591; Bing 1984 *Michigan Yb Int Legal S* 271.

moral sanctions.[198] The Guidelines may also be adopted by private companies on their own instead of by the particular State in which they are located – the USA has opted for this in the private sector.

The second difference lies in the scope of application of the two instruments. While the Guidelines apply to automated and non-automated data files, the Convention's scope is limited to automated files, although it can be extended to include manual files.

The provisions for national and international implementation also differ. The provisions in the Convention are more specific and detailed, thus leaving the members less freedom in the way they implement the principles.

3.5 Council of Europe initiatives following Convention

Since the Convention, the Committee of Ministers of the Council of Europe[199] has issued several "recommendations" on personal data used in automated medical data banks, for scientific research and statistics, for the purpose of direct marketing, for social security purposes, in the police sector, for employment purposes, for payment and related operations, for transfer by the government to third parties, and for personal data used in the area of telecommunications services, with particular reference to telephone services.[200] These documents seek to strengthen data protection in individual member countries, by specifying how the Convention's core principles should apply to specific sectors of data processing activities.[201]

198 They only have "recommendatory effect" (Matthews 1984 *Int Bus L'yer* 410, 411).

199 Also see text to fn 189.

200 For a brief discussion of these recommendations, see Madsen *Personal data protection* 25–26; Ausems "Council of Europe" 541. See also Frosini 1987 *Computer L & Prac* 84, 89.

201 Schwartz 1995 *Iowa L R* 471, 479. Also see Walden "Data protection" 446.

4 EUROPEAN UNION DIRECTIVE ON DATA PROTECTION

The European Parliament and the Council of the European Union adopted Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data in 1995. This document is the most significant international document on data protection to have been published in the last decade.[202] However, the European Community (EC),[203] the forerunner of the European Union (EU), has been involved in data protection for a number of years, and before the Directive itself is analysed, the history of EC involvement in data protection will be examined.

4.1 History of European Community involvement in data protection

The European Community has been involved in the field of data protection since the seventies.
In 1973 the European Commission issued a communication to the Council of the European Communities[204] entitled *Community policy on data processing*.[205] The primary concern of the report

202 See Greenleaf 1995 (2) *Int Priv Bul* 1.

203 The European Community (EC) is a political term that refers to a combination of sixteen Western European countries who have decided that their future well-being lies in economic and political integration. The EC is made up of three Communities, the European Economic Community (EEC), the European Atomic Energy Community (EURATROM) and the European Coal and Steel Community (ECSC). The ECSC was created by the Treaty of Paris in 1951 by six European Countries (France, West Germany, Italy, the Netherlands, Belgium and Luxembourg). Its aim was to form a common market in coal and steel, considered the basic materials of war, in order to give Germany access to these resources, while at the same time preventing any one country gaining control of them. The EEC (also known as the Common Market) was set up by the Treaty of Rome in 1957, and at the same time, by a separate treaty, the third European Community EURATROM was set up. EURATROM focused on joint research and peaceful development of atomic energy (Folsom *European Community law* 7). The executives of the three Communities were merged in 1965 under the Treaty of Brussels, and the term European Community is now taken to include all three Communities. The membership of the EC was enlarged over the years. The aim of the EEC was to achieve a "common market" where goods, services, persons and capital could circulate freely between its members. However, since the mid 1980s the EC's aim has shifted to the attainment of a "single market" by removing physical, technical and fiscal barriers. **Since 1992,** the EC has also been referred to as the **European Union**, after the signing of the Treaty on European Union in Maastricht by the governments of the member countries. Since the Maastricht Treaty, political union has become another aim of the member countries of the EC. See also Archer & Butler *European Community* vi; Mathijsen *European Union law* 3–11; Hill *European Community* 1–6.

204 The EU has four institutions: the European Commission, the Council of European Communities, the European Parliament and the European Court of Justice. The members of the **European Commission** are (continued...)

was the promotion of the European data processing industry,[206] yet it did point out the need to protect the individual against the abuse of computers by third parties.[207]

In contrast, the European Parliament had the protection of the individual as its primary concern right from the start.[208] It took up the point raised by the European Commission on the need for the protection of individuals against the abuse of computers in April 1976, when it passed a resolution in which it

204(...continued)
appointed by the different member states. Each member represents a major policy area. It can be considered to be the civil service or the executive branch of the Community. Although it can be likened to a civil service, it is nevertheless much more than that. It participates in the law-making process of the EC by submitting proposals to the Council. When policies have been decided upon, it sees to their implementation as directives, decisions or regulations (see fn 211). It has a "watch-dog" function and has to monitor whether national agencies or actors are complying with the Treaty obligations and Community legislation. The **Council of the European Communities** (also referred to as the **Council of Ministers**) is the Community legislator. Its task is to ensure coordination of the economic policies of the member states. It consists of delegates from the member states, but is not a fixed body of individuals, its composition depending on the policy in question. (Eg, if agricultural policy is to be discussed, the ministers of agriculture of the member states will attend.) This Council should not be confused with the Council of Europe referred to above in par 3 (Archer & Butler *European Community* 28; Hill *European Community* 7).The **European Parliament** (formerly known as "the Assembly") is a directly elected body of more than 500 members. It is a consultative body, receiving and commenting on Commission proposals before they are adopted. Its participation in the legislative process is limited to issuing an opinion or proposing amendments. The judges of the **European Court of Justice** come from the member states. The Court's judgments are binding throughout the EU. See also Mathijsen *European Union law* 59–162.

205 SEC(73) 4300 final. See Hondius *Emerging data protection* 70; Nugter *Transborder flow of personal data* 29; Campbell *Data transmission and privacy* 150.

206 The Commission stated that the computer industry was expected to become the third largest world industry by 1980, after the automobile and oil industries. The Commission found it disturbing that while the computer industry was crucial for the development of European society, this sector was almost exclusively dependent on American technology. A single American company, IBM, controlled 60% of the European market. The Commission concluded that that was an unhealthy situation and proposed measures to increase the capability of the European data processing industry. See Hondius *Emerging data protection* 69–70; Nugter *Transborder flow of personal data* 29; Campbell *Data transmission and privacy* 150; Simitis 1995 *Iowa L R* 445, 446.

207 Par 39 of the Communication stated:
> The creation of data banks joined increasingly by international links will oblige the Community to establish common measures for protection of the citizen. When police, and tax, and medical records, and files of hire purchase companies concerning individuals are held in data banks, the rules of access to this information become vital... It would be better for the Community to seek a genuine political consensus on this matter now, with a view to establishing common ground rules, than to be obliged to harmonise conflicting national legislation later on.

See Hondius *Emerging data protection* 70.

208 Simitis 1995 *Iowa L R* 445, 446.

instructed its Legal Affairs Committee to investigate and report "on Community activities to be undertaken or continued with a view to safeguarding the rights of the individual in the face of the developing technical progress in the field of automatic data processing".[209] This culminated in May 1979 in a second resolution by the European Parliament.[210] This resolution emphasised the fact that a harmonious development of economic activities within the common market calls for the creation of a genuine common market in data processing. It pointed out that national provisions for protecting privacy have a direct influence on the establishment of this common market. It called on the Community to prepare a proposal for a directive[211] on the harmonisation of legislation on data protection to provide citizens of the Community with the maximum protection.

However, the Commission wanted to await the outcome of the activities of the Council of Europe. When the Council adopted the Convention in 1981,[212] the Commission adopted a resolution encouraging its member states to sign and ratify the Convention before the end of 1982.[213]

In 1982 the European Parliament adopted a Resolution on the Protection of the Rights of the Individual

209 1976 *Official Journal* C 100/27.

210 1979 *Official Journal* C 140/35 (see Nugter *Transborder flow of personal data* 29).

211 Four types of legislation exist in the EU (and previously existed in the EC):
(a) **Directives** are the most important and least common type of rules. Directives are used in the harmonisation of public policy throughout the Union. The goals expressed in directives are binding, but member states are granted some latitude in deciding the actual form of implementation and the detailed content of the legislation – the Directive under discussion is an example of this type of legislation.
(b) **Regulations** have general application and pass into law without further action, eg when Council has set agricultural prices for individual products these prices are published as regulations.
(c) **Decisions** are binding upon whoever they are addressed to and are aimed at individual governments, groups, or individuals.
(d) **Recommendations** and **opinions** have no binding force but can be used to clarify views or issues.
See Archer & Butler *European Community* 38; Mathijsen *European Union law* 25–39; Bennett *Data protection directive* 1.

212 See par 3 above.

213 Recommendation 81/679 981 *Official Journal* L 246 of 29-8-81 (see also Matthews 1984 *Int Bus L'yer* 410, 413).

in the face of Technological Developments in Data Processing.[214] This resolution envisaged a directive on data protection, should the Convention prove to be inadequate.[215]

By 1990 the Convention had been signed by all the Community member states, but ratified by only six.[216] The Commission became concerned at the effect which discrepancies in the member states' laws[217] and regulations might have on inter-community trade,[218] and in 1990 it therefore made proposals for a Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.[219] It was envisaged that this Community legislation should amplify and give substance to the Convention.[220] With the signing of the Maastricht Treaty in 1992,[221] the shift from economic union to political union brought with it new and urgent attention to the protection of citizens' liberties.[222] The Draft Directive was debated by the European Parliament in 1992 and after considerable

214 1982 *Official Journal* C 87/39. This Resolution was the result of a report by the Legal Affairs Committee of the European Parliament. The Legal Affairs Committee examined the Council of Europe Convention, the OECD Guidelines and existing national statutes, and concluded that a Community directive was urgently needed to provide the highest possible level of protection. See Nugter *Transborder flow ofpersonal data* 30–31.

215 Hondius 1983 *Neth Int L R* 103, 105.

216 Denmark, France, Germany, Luxembourg, Spain and the United Kingdom. See Lloyd *Information technology law* 51.

217 For examples of these discrepancies, see Papapavlou "Latest developments" 30.

218 In terms of a 100A of the EC Treaty the aim is to establish a "Single Market". Discrepancies between the data protection laws of member countries were seen as an obstacle to a single European information market (Walden "Data protection" 443–444).

219 1990 *Official Journal* C 277/03; Lloyd *Information technology law* 51.

220 The Convention was the point of departure for the new Community initiatives. It was agreed that all the basic principles of the Convention should be included in the new proposals, but on the other hand it was also felt that they should go further than the Convention, which contained no provisions on liability for damages suffered, on recourse in case of disputes, and on independent supervisory bodies (Papapavlou "Latest developments" 32). In other words, the Directive aims to exceed the level of protection required by the Convention (Greenleaf 1995 (2) *Int Priv Bul* 11).

221 See fn 203.

222 This ideal is expressed in Directive 95/46/EC as follows (recitals par (1)): "... the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the states belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which

(continued...)

amendment,[223] it was finally adopted on 24 October 1995.[224] Member states have three years (twelve years as regards existing manual filing systems) in which to implement the Directive,[225] in other words, by 24 October 1998 member states should have adopted legislation that complies with the provisions of the Directive. Implementation of the Directive may take the form of a either a general law on the protection of individuals as regards the processing of personal data, or sectoral laws, for example those

222(...continued)
divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the member states and in the European Convention for the Protection of Human Rights and Fundamental Freedoms..."

Also see Simitis 1995 *Iowa L R* 445–447 on the importance of this shift.

223 See Simitis 1995 *Iowa L R* 445 *et seq*; Bennett & Raab 1997 *InfSoc* 245, 248; Rosenbaum 1992 *Jurimetrics J* 1. Charlesworth 1999 *Gov Inf Q* 203, 210–211 describes the eventful history of the Directive as follows:

> The European Data Protection Directive had an eventful history; the original draft was put forward by the Commission after unusually limited consultation and received a less than enthusiastic response from some of the member states, notably the UK. It was approved on first reading by the European Parliament, but only after having been subjected to significant amendment. The Commission produced an amended proposal in October 1992, having not only taken on board the European Parliament amendments, but also having considerably restructured the text. Despite this, the amended proposal remained unpopular with a number of Member State governments, notably those of the UK, Ireland, and Denmark, and agreement on the text was to prove unusually difficult to reach. There was intense lobbying throughout this period from various interest groups, most notably the banking and direct marketing sectors, which were, not unnaturally, concerned about the degree of restriction that would be placed on their use of personal data, and about the potential costs of compliance. It is a sign of the initial general unpopularity of the measure that a Common Position was only finally reached in the Council of Ministers on February 20, 1995. However, once this hurdle was finally overcome, the second reading of the emended proposal in the European parliament was relatively uneventful. The Directive was finally adopted in October 1995, five years after its inception and 16 year after the issue of data protection was first raised by the European Parliament.

224 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995 *Official Journal* L 281/31 (hereinafter referred to as "the Directive" and quoted as Dir 95/46/EC).

The Commission's proposal for a general directive in the area of data protection was part of a package of proposals. Also proposed was a Directive Concerning the Protection of Personal Data in the Telecommunications Sector and a Decision in the Field of Information Security (1990 *Official Journal* C 277/18). The information security decision soon came into operation (1992 *Official Journal* L 123/19). After much deliberation, the communications directive was adopted in 1997 (Directive 97/66/EC of the European Parliament and of the Council 1998 *Official Journal* L 24/1). See also par 4.4.

225 Dir 95/46/EC a 32. The Directive is an order to member states of the European Union to amend their laws to comply with the requirements of the Directive (Greenleaf 1995 (2) *Int Priv Bul* 10).

relating to statistical institutions.[226]

4.2 Provisions of Directive[227]

4.2.1 Overview of structure of Directive

The main features of the Directive are:

- Seventy-two Recitals or "whereas..." statements that precede the Directive, explain its purpose and aims, and aid interpretation.[228]

- Chapter I, containing general provisions on the object and scope of the Directive as well as definitions (articles 1–4).

- Chapter II, containing general rules on the lawfulness of the processing of personal data. This chapter has nine sections dealing with the principles relating to data quality, criteria for making data processing legitimate, special categories of data processing, information to be given to the data subject, the data subject's right of access to data, exemptions and restrictions, the data subject's right to object, confidentiality and security of processing and notification to the supervisory authority (articles 5–21).

- Chapter III, dealing with judicial remedies, liability and sanctions (articles 22–24).

---

226 Dir 95/46/EC recitals par (23).

227 For a discussion of the Directive, see Singleton 1995 *Computer L & Prac* 140–144; Cate 1995 *Iowa L R* 431–437; Simitis 1995 *Iowa L R* 445–469; Schwartz 1995 *Iowa L R* 471, 480–488; Greenleaf 1995 (2) *Int Priv Bul* 110–21; Pounder & Kosten 1995 (21) *Data Protection News*; Bennett & Raab 1997 *Inf Soc* 245–255; Trubow 1992 *NW J Int L & Bus* 159; Bennett *Data protection directive*; Swire & Litan *None of your business* 22–49.

228 According to Bennett & Raab 1997 *Inf Soc* 245, 249 the "'whereas statements state intentions, place this Directive in the context of other values and policies, help interpretation and reflect the variety of interests that shaped its content". See also Greenleaf 1995 (2) *Int Priv Bul* 11.

- Chapter IV, stating the rules on the transfer of personal data to third countries (articles 25–26).

- Chapter V, providing for the drawing up of codes of conduct (article 27).

- Chapter VI, requiring the establishment of a supervisory authority in each member state, and setting up a Working Party to attend to the protection of individuals with regard to the processing of personal data (articles 28–30).

- Chapter VII, dealing with the implementation of measures by the Community (article 31).

- Final provisions on how and in what time frame the Directive must be complied with by member states (articles 32–34).

4.2.2 Purpose of Directive

The purpose of the Directive is to reconcile two different and sometimes opposing principles:[229] on the one hand it wants to ensure the **free flow of personal data** between the member states of the European Community,[230] but at the same time it wants to ensure a "**high level of protection**" for the fundamental rights and freedoms of individuals, in particular **the right to privacy**.[231] It aims to achieve this purpose

229 However, Bennett & Raab 1997 *Inf Soc* 245, 249 correctly point out that "harmonized privacy protection legislation" and the free flow of data are "complementing rather than conflicting values".

230 Under EC law the flow of data across national borders within the European Community is regarded as a service, and the free flow thereof may therefore only be restricted on limited grounds, since a 59 of the EC Treaty guarantees the freedom to provide transborder services (Campbell *Data transmission and privacy* 147). Also see Cole 1985 *NYU J Int L & Pol* 893, 928.

The need for the free flow of personal data within the community is expressed in several paragraphs of the recitals of Dir 95/46/EC. See eg Dir 95/46/EC recitals par (3) and (5). Also see recitals par (2), (4) and (6) which emphasize the influence of new telecommunications technology on this issue.

231 See Dir 95/46/EC a 1(1). Fromholz 2000 *Berkeley Tech LJ* 461, 462 states:

> In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. See also recitals par (2) and (10) which emphasize this aim of the Directive. It can thus be stated that the Directive embodies the principle that privacy is a fundamental human

(continued...)

by first of all compelling member states to adopt legislation which conforms to the standards set in the Directive.[232] Minimum and maximum levels of protection are set, but within these levels, the member states can decide for themselves how fundamental rights will be protected.[233] Once the objective of "equivalency"[234] between or "harmonisation"[235] of the data protection laws of the member states has been reached, a prohibition is imposed on member states' inhibiting the free movement of personal data between them on grounds relating to the protection of the rights of individuals.[236]

231(...continued)

right.

Schwartz & Reidenberg *Data privacy law* 2 distil three objectives from the provisions of Dir 95/46/EC: (1) To ensure the rights of individuals and their right to privacy in an information society; (2) to promote the free circulation within the Community of personal data, through the establishment of harmonized protection in all member states; and (3) to prevent the abuse of personal data of Community origin in third countries where adequate protection is not ensured. For a discussion of the issues surrounding the transfer of data to third countries, see par 4.2.7

232 Dir 95/46/EC recitals par (8) provides:

> ... in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all member states; ... this objective is vital to the internal market but cannot be achieved by the member states alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the member states and the need to coordinate the laws of the member states so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; ... Community action to approximate those laws is therefore needed...

233 Dir 95/46/EC a 5. According to Greenleaf 1995 (2) *Int Priv Bul* 11 it is evident from the preamble to the Directive that it should not be seen as a "minimum" standard for privacy laws within the EU, but rather as a consensus between EU states on the "desirable" level of data protection: "It is a standard to be complied with as both the minimum and maximum information privacy protection allowable under EU laws, subject to what the preamble refers to as 'a margin for manoeuver' left to Member States."

234 See Dir 95/46/EC a 30(2).

235 Dir 95/46/EC speaks about "Community action to approximate [data protection] ... laws" of member states (recitals par (8) see fn 232). The terms "approximation" and "harmonisation" of national laws are synonymous. "Harmonisation" is a technical term in European Community law that refers to formal attempts to increase the similarity of legal measures in member nations (Bermann *et al Cases and materials on European Community law* 430 (1993) as quoted in Schwartz 1995 *Iowa L R* 471, 481 fn 69). On the inherent difficulties in harmonisation of national laws, see Simitis 1995 *Iowa L R* 445, 449–452.

236 Dir 95/46/EC a 1(2) provides that "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1". (A 1 par 1 provides that member states must protect the fundamental rights and freedoms of natural persons (see fn 231).) This consequently does away with member states' rights under Convention 108/1981 to halt the flow of data across their boundaries on the ground that it is necessary to protect their citizens' rights (Pounder & Kosten 1995 (21) *Data Protection News* 5). Also see Dir 95/46/EC recitals par (9).

4.2.3 Scope of Directive

The Directive applies to the **processing** of **personal data** of a **data subject** by **automatic or nonautomatic means** by a **controller**.

Personal data are broadly defined as any information[237] relating to an identified or identifiable natural person, known as the **data subject**, and **processing of data** equally broadly includes any operation performed upon personal data.[238] The **controller** is the natural or juristic person, public authority, agency or other body which determines the purposes for which and the means by which the data are processed.[239]

---

237 Dir 95/46/EC a 2(a). The drafters of the Directive were of the opinion that any item of data relating to an individual, harmless though it may seem, may be sensitive (eg a mere postal address). See the first draft of the Directive in Commission of the European Communities Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data COM (90) final – SYN 287 Brussels September 1990 Explanatory Memorandum 19.

238 Dir 95/46/EC does not in general distinguish between the different stages of processing of data, ie collection, use and disclosure, but defines processing of personal data in a 2(b) as

> "... any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

This reflects the fluid and decentralised information highway environment of the 1990s (see text to footnote 254).

Pounder & Kosten 1995 (21) *Data Protection News* 7 emphasise that "[i]n Directive terms, 'processing' has no limits; it could be any action performed on personal data". Berkvens 1995 *Computer L & Prac* 38–44 is critical of the broad definitions of "personal data" and "processing". He argues that these broad definitions will result in data protection laws being applied to situations which they were not originally intended for, viz where personal data are processed solely by reference to objects, and not by reference to the data subjects. However, because it has technically become increasingly easier to link personal data to object data, the processing will now come within the scope of the definitions. Because "processing" does not exclude "transmission" of messages, intermediate service providers could also be held responsible for the content of messages they are transferring, even though they do not even know what the content of the messages is.

239 Dir 95/46/EC a 2(d) defines a "controller" as meaning "... the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law..."

When personal data are sent in an e-mail message, the controller in respect of the personal data will be considered to be the person from whom the message originates, rather than the person offering the transmission services (Dir 95/46/EC recitals par (47)).

Where the processing is by **nonautomatic means**,[240] the personal data must form part of a filing system, or be intended to form part of such a system,[241] that allows for access to the personal data according to specific criteria.[242] The Directive also applies to **sound and image data** (for example video surveillance data)[243] relating to natural persons, provided the processing of such data is automated or the data are contained (or are intended to be contained) in a filing system structured according to specific

240 The UK was opposed to the inclusion of manual files in the scope of the Directive (see Greenleaf 1995 (2) *Int Priv Bul* 11). The provenance of this provision is the German Federal Data Protection Act (Bundesdatenschutzgesetz) of 1993 (Jay & Hamilton *Data protection* 23). The following arguments have been advanced in support of the fact that a distinction should not be made between automatic and non-automatic processing:

– If manual processing is not included, data controllers might use manual processing to circumvent data protection obligations.
– A distinction might create a disincentive for the use of new technologies.
– It could undermine fair competition if similar enterprises in the same markets, but using different techniques, were subject to different obligations.
– Data subjects would find it difficult to understand that their rights depend on whether their personal data were recorded electronically or not.

(See House of Lords Select Committee *Report on protection of personal data* 1993 par 35). Dir 95/46/EC recitals par (27) also refer to the serious risk of circumvention if manual processing is excluded.

Member states have a longer time to comply with the Directive in the case of manual files. In general, they must comply with the provisions of the Directive within three years after its adoption. However, in the case of the processing of data **already held** in **manual** filing systems at that time (ie 24 October 1995), the Member Countries have twelve years to comply with most of the provisions of the Directive. However, if they continue to process the data in such manual filing systems during the extended period, they must bring the filing system into conformity with the provisions of the Directive at the time of such processing (Dir 95/46/EC recitals par (69)). Furthermore, the data subject may not be denied his or her right of access and rectification in the extra nine years (Dir 95/46/EC a 32(2)).

241 Dir 95/46/EC a 3(1).

242 A "personal data filing system" is defined in a 2(c): as " any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis". This definition is thus based on the criterion of possibility of access to the personal data.

Dir 95/46/EC recitals par (27) also makes it clear that the Directive covers only manual processing where structured files are involved, and that the files should furthermore be structured according to specific criteria relating to individuals, allowing easy access to personal data. The UK, Denmark and Ireland were opposed to the inclusion of structured manual files in the scope of the Directive (Greenleaf 1995 (2) *Int Priv Bul* 11).

243 Dir 95/46/EC recitals par (14) states:

> ... given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data....

However, note that video surveillance tapes made for public security or criminal law activities, will be excluded. See fn 251 and accompanying text. Also important to note is that the principles of the Directive are to be applied in a restrictive manner when audiovisual material can be considered to be literary or artistic expression, or relates to journalism (see Dir 95/46/EC a 9 and recitals par (17)).

criteria relating to individuals, so as to permit easy access to the personal data in question.[244]

Only **natural persons** can be data subjects, since a data subject is by definition "an identifiable natural person".[245] The privacy rights of juristic persons are thus not protected by the Directive.[246]

No distinction is made between the processing of data in the **private or public sectors**, and the Directive applies equally to both areas.[247]

The Directive does **not apply**[248] to the processing of personal data by a natural person for purely personal or domestic activities,[249] and neither does it apply to the processing of personal data in the

244 Dir 95/46/EC recitals par (15).

245 Dir 95/46/EC a 2(a). An "identifiable person" is defined as "... one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". Some commentators argue that this definition also includes dead persons (see House of Lords Select Committee *Report on protection of personal data* 1993 par 26; Pounder & Kosten 1995 (21) *Data Protection News* 6; Cate *Information age* 36), but Dutch commentators have an opposite view (see Berkvens & Prins *Van WPR naar WBP* 326). What is clear, however, is that the principles of protection do not apply to anonymous data (Dir 95/46/EC recitals par (26)).

246 See also 95/46/EC recitals par (24).

247 One should remember that the EC's area of competence is the private sector, or the market, and not the public sector, (see Simitis 1995 *Iowa L R* 445 452; Schwartz 1995 *Iowa L R* (Panel Discussion) 683) and one may have expected that the Directive would distinguish between the two areas. In fact, a distinction was initially drawn in the first draft of the Directive as regards the fair obtaining and legitimacy of the processing of data (see fn 237, 247). See also Bennett *Data protection directive* 8. However, it was realised that it is not possible to separate the private and public sector. Simitis 1995 *Iowa L R* 445, 452 explains:

> Patients in a private clinic are, as far as the use of their data is concerned, in the same situation as those treated in a hospital belonging to the state. Employees are confronted by the same problems with respect to their data whether they are employed by a computer firm or by a tax authority. The implications of processing for customers do not change because a bank is, as in many Member States, owned by the state and organized in a form typical of state activities.

248 Dir 95/46/EC a 3(2).

249 The rationale for the "domestic purposes" exclusion is that invasion of privacy is unlikely to occur. According to Pounder & Kosten 1995 (21) *Data Protection News* 9 this exception is necessary to comply with a 8 of the European Convention on Human Rights which calls for respect of family life.

The first draft (see fn 237, 247) also excluded the files of non-profit making bodies, because it could be presumed that the members of such bodies consented to being in the files. However, the final Directive does not contain such an exception.

course of an activity which falls outside the scope of Community law,[250] for example processing operations related to public security, defence, state security, and the areas of criminal law.[251]

4.2.4 General rules on lawfulness of processing of personal data[252]

The Directive lays down general rules determining under what circumstances personal data may lawfully be processed. The member states must determine more precisely the specific conditions that must be adhered to.[253]

Traditionally, there has always been a distinction in data protection laws or international instruments between limitations on collection, limitations on use, and limitations on disclosure of data. However, reflecting the "more fluid and decentralised 'information highway' environment of the 1990s,"[254] the Directive does not emphasise the distinction between collection, use or disclosure of data, but speaks more generally about "data processing".[255] It therefore does not distinguish between limitations on the different stages of processing either, but provides that member states must, within the limits of the Directive, determine "the conditions under which processing of personal data is lawful".[256]

4.2.4.1 Principles relating to data quality

250 Swire & Litan *None of your business* 27 argue that the result of this exemption is to focus the Directive "primarily on the private sector".

251 Video surveillance tapes that were made for any of these purposes will consequently also be excluded from the Directive.

252 These rules reflect the "fair information principles" or "data protection principles" found in data protection documents (see eg par 2.2.5). They consist on the one hand of obligations imposed on persons, public authorities, enterprises, agencies and other bodies responsible for processing data, and on the other hand they refer to the rights conferred on individuals (Dir 95/46/EC recitals par (25), Schwartz & Reidenberg*Data privacy law* 13).

253 Dir 95/46/EC a 5.

254 Bennett *Data protection directive* 5; Bennett & Raab 1997 *Inf Soc* 245, 250.

255 See also fn 238.

256 Dir 95/46/EC a 5. From this, one can deduce that the processing of personal data which does not come within these limits is *per se* unlawful.

Personal data must be processed fairly and lawfully.[257] Specifically, personal data must be collected for "specified, explicit and legitimate" purposes and must not undergo further processing in a way incompatible with those purposes.[258] As will be demonstrated, this "purpose specification" principle is the linchpin around which many of the other provisions turn.[259] The purpose for which data are collected must be determined at the time of collection, and must be made known to the subject at that time.[260] This purpose must be a legitimate one. Further processing of data that is incompatible with this purpose is not allowed.[261] Processing for historical, statistical and scientific purposes will not be considered to be incompatible,[262] provided that the member states lay down appropriate safeguards.[263]

257 Dir 95/46/EC a 6(1)(a).

258 Dir 95/46/EC a 6(1)(b).

259 Bennett *Data protection drective* 4.

260 Dir 95/46/EC recitals par (28).

261 This principle is also known as the "finality" principle or concept (see Bennett *Data protection directive* 4; Pounder & Kosten 1995 (21) *Data Protection News* 12).

262 Processing of data for research purposes is generally treated more favourably than other data processing activities. Simitis 1995 *Iowa L R* 445, 457 explains why:

> To a considerable extent, research presupposes a deliberate disregard of the goals for which the data were originally collected. In order to successfully conduct their research, cardiologists evaluating the effectiveness of different drugs, historians studying the involvement of different persons in a particular political development, sociologists analysing the role of welfare agencies, and criminologists investigating the family background of juvenile delinquents must have access to a substantial amount of data provided by the persons concerned in a different context and for clearly different reasons.

Simitis (458) argues that more lenient restrictions for research projects should be linked to two important conditions: (a) data subjects must as a rule fully retain their rights (eg, that they should consent to the processing and their right to correct information), and (b) data obtained for research purposes must be inaccessible for any other use outside of research. Simitis (458) considers the Directive to be too lenient is this respect, since it merely provides that member states should introduce "appropriate safeguards" to reduce the risks ensuing from eg a change of purpose (a 6(1)(b)) or from not informing the data subject (a 11(2)). Also see Simitis 1981 *Am J of Comp L* 583.

263 These safeguards must in particular rule out the use of the data "in support of measures or decisions regarding any particular individual"(Dir 95/46/EC recitals par (29)).

It is further provided that personal data must be "adequate, relevant and not excessive,"[264] must be "accurate", complete and "kept up to date",[265] and must not be stored in a form which permits identification of data subjects for longer than is necessary. Member states must lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[266] The adequacy, relevance, accuracy and up-to-dateness of the data are once more determined with reference to the purpose for which they have been collected or further processed. "Every reasonable step" must be taken to rectify or erase inaccurate, incomplete and outdated data.[267]

The responsibility is placed on the controller to ensure that data are processed fairly and lawfully, and that the data quality principles are complied with.[268]

Member states may restrict the scope of the rights and obligations provided for by the data quality principle, when such a restriction constitutes a necessary measure to safeguard certain public interests,[269] or to protect the data subject or the interests of others.[270]

4.2.4.2 Criteria for making data processing legitimate

Apart from the principles relating to the quality of the data, the Directive also spells out the **only** six conditions under which personal data may lawfully be processed:

---

264 Dir 95/46/EC a 6(1)(c).

265 Dir 95/46/EC a 6(1)(d).

266 Dir 95/46/EC a 6(1)(e). See also fn 262.

267 Dir 95/46/EC a 6(1)(d).

268 Dir 95/46/EC a 6(1)(a) and 6(2).

269 Namely national security, defence, public security, criminal investigations, investigations of breaches of ethics for regulated professions, important economic or financial interests of a member state or of the European Union.

270 Dir 95/46/EC a 13(1).

- ❒ The data subject has unambiguously consented.[271]

- ❒ Processing is necessary for the performance of a contract to which the data subject is party (or to complete a precontractual stage at the request of the data subject).[272]

- ❒ Processing is necessary for compliance with a legal obligation to which the controller is subject.[273]

- ❒ Processing is necessary in order to protect the vital interests of the data subject.[274]

- ❒ Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.[275]

- ❒ Processing is necessary for the "legitimate interests" of the controller or third parties to whom

271 Dir 95/46/EC a 7(a). "The data subject's consent" is defined in a 2(h) as meaning "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." Implied consent is not sufficient (see Pounder & Kosten 1995 (21) *Data Protection News* 8). Consent can be withdrawn at any time (Madsen *Personal data protection* 27). The consent must be "unambigous". This means that the controller must have no doubt about the fact that the data subject has consented. The onus is on the controller to ensure that the data subject has consented (WBP *Memorie van toelichting* 66).

272 Dir 95/46/EC a 7(b).

273 Dir 95/46/EC a 7(c).

274 Dir 95/46/EC a 7(d). "Vital interest" is described in the recitals par (31) of Dir 95/46/EC as "an interest which is essential for the data subject's life". As a consequence this provision will probably have limited application (see Pounder & Kosten 1995 (21) *Data Protection News* 14).

275 Dir 95/46/EC a 7(e). Member states must determine whether the controller performing a task carried out in the public interest or in the exercise of official authority must be a public administration or another natural or juristic person governed by public law, or by private law such as a professional association (see Dir 95/46/EC recitals par (32)).

the data are disclosed,[276] except where such interests are overridden by the data subject's interests in his or her "fundamental rights and freedoms" which are protected by the Directive.[277]

Data subjects must have the right to object to the processing of data relating to them, at least as regards the processing of data necessary for the performance of a task carried out in the public interest or in the exercise of official authority, and as regards the processing of data that is in the "legitimate interests" of the controller or third parties to whom the data are disclosed.[278]

4.2.4.3 Special categories of processing

a Sensitive data

Member states must prohibit the processing of personal data that are considered to be of a "sensitive" nature.[279] The category of sensitive data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health[280] or sex life.[281]

276 According to Dir 95/46/EC recitals par (30) member states may determine the circumstances under which data may be used or disclosed to a third party "in the context of the legitimate ordinary business activities of companies and other bodies". Member states may also specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing, be it by a commercial or charitable organization or by eg a political organisation. In both these instances, however, the data subject must be granted a right to object to the processing (Dir 95/46/EC a 14) See also fn 325.

277 Dir 95/46/EC a 7(f).

278 On the right to object, see par 4.2.4.7.

279 In other words, personal data that are by their nature capable of infringing fundamental freedoms or privacy (see Dir 95/46/EC recitals par (33)). This provision originates from French and Belgian law. However, not everybody agrees that data can be sensitive by nature. Many data protection advocates would argue that any data can become sensitive depending on the circumstances (eg, a last name may reveal ethnic origin or even religious beliefs), and that so-called "sensitive" data may be innocuous in certain situations. This provision is inconsistent with the German view eg that "sensitivity" depends on the particular processing context. Names and addresses in a telephone directory can be innocuous, but names and addresses in connection with lists indicating the inmates of psychiatric hospitals are definitely sensitive (see Simitis 1995 *Iowa L R* 445 450 fn 35).

280 The prohibition does not apply where the processing of the data is required 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 competent national bodies, under the obligation of professional secrecy or by another (continued...)

However, this commendably strict provision is watered down by a list of exceptions which was inserted in the final draft of the Directive at the insistence of some of the member states.[282]

Processing of sensitive data may be permitted[283] by member states if:

- the data subject has explicitly consented[284] thereto[285]
- the processing is necessary for the data controllers to carry out their obligations in the field of employment law[286]
- the processing is necessary to protect the vital interests of the data subject or those of another person where the data subject is physically or legally incapable of giving his or her consent[287]
- the processing is carried out by a foundation, association or any other non-profitseeking body

280(...continued)
person also subject to an equivalent obligation of secrecy (Dir 95/46/EC a 8(3)).

281 Dir 95/46/EC a 8(1).

282 Simitis 1995 *Iowa L R* 445, 460–461. Simitis does not think that all the exceptions are justified.

283 It is not compulsory to insert all or any of these exemptions into national laws. A member state may have "stricter" rules than those prescribed by the Directive, but may not stop the free flow of data for this reason.

284 An earlier draft required "written" consent, but in the final draft the requirement that consent must be in writing has been left out. For the definition of "consent" see fn 271. "Explicit" consent is required. Implied consent is not sufficient. The data subject should make it clear in words, writing or conduct that she consents to the processing of personal data (WBP Memorie van toelichting 65).

285 However, the laws of the member state may also provide that the prohibition may not be lifted by the data subject's consent (Dir 95/46/EC a 8(2)(a)).

286 Dir 95/46/EC a 8(2)(b). A member state must provide "adequate safeguards" in such a case.

287 Dir 95/46/EC a 8(2)(c).

for political, philosophical, religious or trade-union purposes[288]

- ❒ the processing relates to data which are manifestly made public by the data subject[289]

- ❒ the processing is necessary for the establishment, exercise or defence of legal claims[290]

Member states may also "for reasons of substantial public interest"[291] lay down additional exemptions, provided that "suitable safeguards" are introduced[292] and provided that the member state notifies the Commission of such exemptions.[293]

b Data on criminal offences

Processing of data that pertain to criminal offences, convictions and security measures may only be carried out under the control of an official authority, unless a derogation is made to this rule in national law providing "suitable specific safeguard".[294] In this instance the Commission must also be notified of

288 Dir 95/46/EC a 8(2)(d). The processing by such a body must be in the course of its legitimate activities, with appropriate guarantees, and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subject.

289 Dir 95/46/EC a 8(2)(e). An example would be where a person reveals his or her preference for a specific political party in a newspaper (Pounder & Kosten 1995 (21) *Data Protection News* 14).

290 Dir 95/46/EC a 8(2)(e).

291 Dir 95/46/EC recitals par (34) give examples of such "substantial public interests", namely public health and social protection, scientific research and government statistics. Furthermore, religious associations and political parties may also process data on important public grounds. "Official authorities" of "officially recognised religious associations" may process personal data to achieve aims "laid down in constitutional law or international public law" (recitals par (35)). Political parties may compile data on people's political opinion in the course of electoral activities (recitals par (36)).

292 Dir 95/46/EC a 8(4).

293 Dir 95/46/EC a 8(6). The exemptions may be laid down in national law or by the supervisory authority.

294 Britain was of the opinion that prospective employers and grantors of credit and insurance should be allowed to keep information about criminal convictions (House of Lords Select Committee *Report on protection of personal data* 1993 par 139).

the derogation.[295] However, a complete register of criminal convictions may only be kept by an official authority.[296] Member states may provide that data relating to administrative sanctions or judgments in civil cases must also be processed under the control of official authority.[297]

c National identification number

The use of a national identification number is not prohibited, but it is left to member states to determine the conditions under which such a number may be processed.[298]

4.2.4.4 Processing of data and freedom of expression

Member states must make provision for exemptions or derogations from the provisions relating to the lawfulness of processing, the rules relating to the transfer of data to third countries, and the provisions relating to the supervisory authority and the Working Party established by the Directive, where personal data are processed solely for journalistic purposes or the purpose of artistic or literary expression, if they are necessary in order to reconcile the right to privacy with the rules governing freedom of expression.[299]

---

295 Dir 95/46/EC a 8(5) and 8(6).

296 Dir 95/46/EC a 8(5).

297 Dir 95/46/EC a 8(5).

298 Dir 95/46/EC a 8(7).

299 Dir 95/46/EC a 9. This provision is necessary in order for the Directive to give effect to a 10 of the European Convention on Human Rights, which declares that "everyone has the right to freedom of expression"; this right includes the right "to receive and impart information". The member states may, however, not lay down exemptions from the security principle (see par 4.2.4.9). The provisions of a 9 naturally also apply to the processing of sound and image data carried out for journalistic purposes, or for literary or artistic expression (Dir 95/46/EC recitals par (17)). Britain was opposed in principle to such a provision. Their view was that the right of free information and expression is not a special prerogative of the media, but is available to everyone, and the media must not be given special exemptions either at Community level or at national level. In the UK no special privilege was given to the media to grant them freedom of expression. It was also felt that the media are capable of doing the gravest damage if they infringe the right to privacy (House of Lords Select Committee *Report on protection of personal data* 1993 par 142).

4.2.4.5 Duty to inform data subjects

Member states must ensure that the data controllers provide the data subjects with certain information.[300] The data subjects must at least be informed about the identity of the controllers and of their representatives, and the purposes of the processing for which the data are intended. Further information such as the categories of data concerned,[301] the recipients of the data, whether replies to the questions are obligatory or voluntary, the possible consequences of failure to reply,[302] and the existence of the right of access to data and the right to rectify such data if they are incorrect,[303] must be supplied "in so far as it is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing" in respect of the data subjects.[304]

Where the data are collected from the data subjects, the above-mentioned details must be given to them at the time of the collection, except if they are already familiar with such details.[305] Where the data have not been obtained from the data subjects, the details must be given to them at the time of the recording of the data, or at the latest when the data are disclosed to third parties for the first time, unless the data subjects are already familiar with such details.[306]

Where the data have not been collected from the data subjects, the requirement that information must be given to the data subjects does not apply in the following instances:

- where, in particular in the case of processing for statistical purposes or for the purposes of

300 Dir 95/46/EC a 10 and 11(1). Processing of data cannot be fair unless the data subject is in a position to learn of the existence of a processing operation (see Dir 95/46/EC recitals par (38)).

301 Where the data have not been collected from the data subject personally (Dir 95/46/EC a 11(1)).

302 Where the data are collected from the data subject personally (Dir 95/46/EC a 10).

303 See par 4.2.4.6.

304 Dir 95/46/EC a 10 and 11(1).

305 Dir 95/46/EC a 10.

306 Dir 95/46/EC a 11(1).

historical or scientific research,[307] the provision of such information proves impossible,[308] or would involve a disproportionate effort[309]

❒ if recording or disclosure is expressly required by law

In these circumstances member states must provide appropriate safeguards.[310]

Member states may restrict the rights and obligations as regards the duty to inform the data subjects, when such a restriction constitutes a necessary measure to safeguard certain public interests,[311] or to protect the data subjects or the interests of others.[312]

4.2.4.6 Data subjects' right of access to data

The right of access provided for in article 12 can better be described as the right to participate in the data processing process,[313] since it falls into three parts. It requires member states to guarantee first of

307 Processing of data for research purposes is generally treated more favourably than other data processing activities. See also fn 262.

308 Eg because the address of the data subject is not known (Pounder & Kosten 1995 (21) *Data Protection News* 19).

309 Pounder & Kosten 1995 (21) *Data Protection News* 19 indicate that the word "disproportionate" can relate to one of two things: either to the **effort involved** (ie unreasonable demands are made on the controller), or to the **purpose of the Directive** (if the recording or disclosure involved was unlikely to harm the data subject, then provision of this information could be claimed to be disproportionate to that aim).

Factors that can be taken into consideration in this regard are the number of data subjects, the age of the data and any compensatory measure adopted (Dir 95/46/EC recitals (par 40)).

310 Dir 95/46/EC a 11(2). For criticism of the "appropriate safeguards" provision, see Simitis 1995 *Iowa L R* 445, 458 and fn 262.

311 Namely national security, defence, public security, criminal investigations, investigations of breaches of ethics for regulated professions, important economic or financial interests of a member state or of the European Union.

312 Dir 95/46/EC a 13(1).

313 See eg the OECD Guidelines' individual participation principle described in par 2.2.5.7.

all that every data subject has the right of **access** to data relating to the data subject personally[314] "without constraint", "at reasonable intervals" and "without excessive delay or expense"; secondly that data which are incomplete or inaccurate, or the processing of which otherwise does not comply with the provisions of the Directive, be **rectified, erased or blocked**;[315] and thirdly that **third parties** to which data have been disclosed must **be notified** of any subsequent rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort.[316]

The first right in this article, namely the right to access data, can be broken down into three separate rights, namely:

- the right of the data subjects to obtain confirmation as to whether or not data relating to them are being processed as well as information at least on the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed

- the right to obtain, in an intelligible form, the data undergoing processing and any available information as to their source

- the right to obtain knowledge of the logic involved in any automatic processing of data concerning the data subject (at least in the case of the automated decisions)[317]

The scope of the rights and obligations provided by article 12 may be restricted by member states, if

314 Dir 95/46/EC a 12(a). This is an essential provision because it is only through individual access that the accuracy of the data and the lawfulness of the processing can be established (Dir 95/46/EC recitals par (41); House of Lords Select Committee *Report on protection of personal data* 1993 par 131).

315 Dir 95/46/EC a 12(b).

316 Dir 95/46/EC a 12(c). On the meaning of "disproportionate" see fn 309.

317 See Dir 95/46/EC a 15(1). This provision should not be interpreted so as to adversely affect trade secrets or intellectual property rights, such as copyright protecting software (see Dir 95/46/EC recitals par (41)). This provision derives from French law. It has been claimed that it will cause considerable difficulties to US companies (Greenleaf 1995 (2) *Int Priv Bul* 13).

such restriction constitutes a "necessary measure" to safeguard certain public interests,[318] or to protect the data subject or the interests of others.[319] Member states may also restrict the rights provided by article 12 when data are processed solely for purposes of scientific research[320] or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics. Two provisos are added to the last exception: member states must provide "adequate legal safeguards"[321] in particular "that the data are not used for taking measures or decisions regarding any particular individual". It is also provided that there must clearly be "no risk of breaching the privacy of the data subject".[322]

The restrictions on the right of access are not mandatory. Member states must determine for themselves, against the background of the Directive, whether it is necessary to impose any restrictions.[323]

---

318 Namely national security, defence, public security, criminal investigations, investigations of breaches of ethics for regulated professions, important economic or financial interests of a member state or of the European Union. In earlier drafts of the Directive the Commission proposed that it should be required that the member state's interest must be "a duly established paramount interest". This was watered down in the final form of the Draft (see Simitis 1995 *Iowa L R* 445, 459).

319 Dir 95/46/EC a 13(1). It would eg be permissible to specify that access to medical data may be obtained only through a health professional (Dir 95/46/EC recitals par (42)).

320 As indicated, data processed for research purposes are in a favoured position (see fn 262).

321 On the appropriate safeguards provision, see fn 262.

322 Dir 95/46/EC a 13(2).

323 Simitis 1995 *Iowa L R* 445, 460 is of the view that the Commission and the Council chose the wrong approach in this regard, and that they must have laid down rules which clearly state that the data subject's right to access can never be totally excluded, but can at most be partially restricted or temporarily suspended in a series of unequivocally defined and specifically listed cases. He argues:

> The refusal of the Commission and of the Council to directly regulate the restrictions, however, can hardly be defended, especially in view of the experiences of the Member States. The governments of the Member States had never particularly welcomed the data subjects' right to know. Their primary concern was not to secure this right, but rather to protect the public authorities against the exercise of a right perceived to be a serious threat to their efficiency. Credit for the gradual improvement of the right to access goes, therefore, entirely to courts and parliaments. Without their constant corrective interferences, the right to know would be largely fictitious.

4.2.4.7 Data subjects' right to object

Data subjects must have the right to object to the processing of data relating to them, at least as regards the processing of data necessary for the performance of a task carried out in the public interest or in the exercise of official authority, and as regards the processing of data that is in the "legitimate interests" of the controller or third parties to whom the data are disclosed.[324] The grounds for objection must be "compelling legitimate grounds" relating to the data subject's particular situation, unless otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve the data objected to.[325]

The right to object to the processing of data must also exist where data are processed for direct marketing purposes, at no cost and without having to give reasons.[326] Member states are given the responsibility for taking the necessary measures to ensure that data subjects are aware of the existence of the right to object to the processing of data for direct marketing purposes.[327]

4.2.4.8 Automated individual decisions

Article 15 of the Directive provides that member states must grant every person the right not to be subjected to a decision which produces legal effects concerning or significantly affecting that person,

---

324 See par 4.2.4.2.

325 Dir 95/46/EC a 14(a).

326 Dir 95/46/EC a 14(b). As Bennett *Data protection directive* 5 points out, the Directive makes clear that data subjects must have the right to object to the processing of personal data for direct marketing purposes. However, the mechanism, ie whether an "opt-in" or "opt-out" system should be used, is not prescribed. (With an "opt-in" system, the data subjects must specifically be asked whether they want to be included before their data may be processed lawfully. With an "opt-out" system, the data subjects should object if they want their names to be removed from a direct marketing list.)

A 14(b) provides that "Member States shall grant the data subject the right: ... (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses."

327 Dir 95/46/EC a 14(b).

and which is based solely on automated processing of data intended to evaluate certain related personal aspects, such as for performance at work, creditworthiness, reliability, and conduct.[328] Exceptions may be provided for where the decision is taken in the context of a contract or where it is authorised by law, provided that the subject's legitimate interests are safeguarded.[329]

Article 15 is an unusual data protection provision in two ways: First, less than a handful of countries had this type of provision in their data protection laws before the Directive,[330] and second, its focus is not on data processing, but on a type of decision making. Examples of this type of decision making, referred to as "automated profiling",[331] are the listing of applicants for a job in order of preference solely on the basis of a test of personality, and the use of scoring techniques for the purpose of assessing creditworthiness.[332]

Article 15 is designed to protect the individual against the perceived growth of automatisation of organisational decisions about individuals. According to Bygrave,[333] the drafters of the Directive were

328 Dir 95/46/EC a 15.

329 Dir 95/46/EC a 15(2)(a) and (b).

330 This provision originates from French law (House of Lords Select Committee *Report on protection of personal data* 1993 par 66). Bygrave 2001 *Computer L & Sec Rep* 17 points out that apart from the French, only the Spanish and Portuguese data protection laws incorporated similar provisions.

331 Bygrave 2001 *Computer L & Sec Rep* 17 describes profiling as follows: "Generally speaking profiling is the process of inferring a set of characteristics (typically behavioural) about an individual person or collective entity and then treating that person/entity (or other persons/entities) in the light of these characteristics. As such, the profiling process has two main components: (i) profile generation – the process of inferring a profile; (ii) profile application – the process of treating persons/entities in the light of this profile. The first component typically consists of analysing personal data in search of patterns, sequences and relationships, in order to arrive at a set of assumptions (the profile) based on probabilistic reasoning. The second component involves using the generated profile to help make a search for, and/or decision about, a person/entity. The line between the two components can blur in practice, and regulation of the one component can affect the other component." Also see ch 1 par 1.2.

332 House of Lords Select Committee *Report on protection of personal data* 1993 par 66.

333 Bygrave 2001 *Computer L & Sec Rep* 17, 18 says:

> One can read into [the comments of the drafters] a concern that, in the context of organizational decision making, the registered data images of persons (their 'data shadows') threaten to usurp the constitutive authority of the physical self despite their relatively attenuated and often

(continued...)

concerned about the diminished role played by persons in shaping important decision-making processes that affect them.[334] Note that article 15 does not prohibit the creation of profiles,[335] it only imposes restriction on their application.[336] For example, profiling may be done as long as individuals are given the opportunity to exercise a right to object to such decision making.

For the right contained in article 15(1) to apply, four cumulative conditions must be satisfied:[337]

- A decision must be made.

  Making a decision about someone usually entails adopting a particular attitude or stance towards that person. This could result in denying a request or in taking action that will have an influence on the person. According to Bygrave,[338] a decision ordinarily connotes a mental action, that is, the adoption of a particular opinion or belief.

- The decision concerned must have legal or otherwise significant effects on the person who is the subject of the decision.

  Legal effects are effects that are able to alter or determine a person's legal rights or duties. It is more difficult to interpret the meaning of "significant effect". The sending of a commercial brochure to a person selected by a computer will probably not have a significant effect on the

333(...continued)
misleading nature. A further concern is that this threat brings with it the threat of alienation and a threat to human dignity.

334 It can of course also be argued that automated decisions could sometimes be fairer to individuals than a personal judgement (House of Lords Select Committee *Report on protection of personal data* 1993 par 70).

335 National legislators are not prevented from implementing this section in a way that imposes a ban on profiling (Bygrave 2001 *Computer L & Sec Rep* 17, 18).

336 Bygrave 2001 *Computer L & Sec Rep* 17, 18.

337 See Bygrave 2001 *Computer L & Sec Rep* 17, 18. Also see Cate *Information age* 39–40.

338 2001 *Computer L & Sec Rep* 17, 19.

person and will therefore not fall under the prohibition imposed by this section. In other situations it may be more difficult to decide on the significance of a decision.[339]

❒ The decision must be based solely on automated data processing.[340]

Bygrave[341] is of the opinion that the notion "solely" seems intended to denote "a situation in which a person fails to actively exercise any real influence on the outcome of a particular decision-making process. Such a situation would exist if a decision, though formally ascribed to a person, originates from an automated data-processing operation the result of which is not actively assessed by either that person or other persons before being formalised as a decision".

❒ The data processed must be intended to evaluate certain personal aspects of the person who is the subject of the decision.

The phrase "certain personal aspects" is ambiguous. The phrase undoubtedly refers to aspects of the data subject's person or personality. The inclusion of the word "certain" indicates, however, that not all personal aspects are legally relevant for the application of article 15(1). As has been demonstrated, the article lists examples of legally relevant personal aspects, namely aspects that concern performance at work, creditworthiness, reliability, and conduct. In other words, they must concern a person's character.[342] Article 15(1) would not apply for example to a fully automated decision by a bank to refuse a person cash simply because the person lacks the necessary credit in his or her bank account. However, if the decision concerned were

339 Bygrave 2001 *Computer L & Sec Rep* 17, 19 points to the following problem areas: "Does the notion refer only to effects that are significant for the data subject in an objective sense (ie, relatively independent of the data subject's own perceptions)? Does it refer only to effects of a material (eg economic) nature? Does it require the decision concerned to be adverse to the interests of the data subject?". Also see Cate *Information age* 39–40.

340 Ie, there must be strict application of the results produced by the computer.

341 Bygrave 2001 *Computer L & Sec Rep* 17, 20.

342 Bygrave 2001 *Computer L & Sec Rep* 17, 20.

> grounded on a fully automated analysis of the person's payment history; article 15 would be applicable.[343]

Bygrave points to the following difficulties in implementing article 15: the complexity and numerous ambiguities in the way its provisions are formulated; the paucity of authoritative guidance on the scope and application of the provisions; and the fact that the article's application is contingent upon a large number of conditions being satisfied. However, he concludes that:

> Art 15 is normatively important in terms of the principle it establishes and embodies. This principle is that fully automated assessments of a person's character should not form the sole basis of decisions that significantly impinge upon the person's interests. The principle provides a signal to profilers about where the limits of automated profiling should roughly be drawn.[344]

4.2.4.9 Confidentiality and security of processing

The Directive aims to ensure the confidentiality of processing by requiring member states to prohibit the processing of data by any person who has access to it, unless such person has been instructed to do so by the controller or required to do so by law.[345]

Member states must also spell out the responsibilities of the controller in regard to security measures. The controller must implement appropriate technical and organisational measures to protect personal data from accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and from all other unlawful forms of processing.[346] The measures must ensure a level of security that is appropriate to the risks presented. Factors that are relevant in determining the appropriateness of the measures are

343 Bygrave 2001 *Computer L & Sec Rep* 17, 20.

344 Bygrave 2001 *Computer L & Sec Rep* 17, 20.

345 Dir 95/46/EC a 16.

346 These measures must be implemented both at the design stage of the processing system and at the time of processing itself (Dir 95/46/EC recitals par(46)).

the state of the art, the cost of implementation, and the nature of the data to be processed.[347]

Should the controller choose a processor to do the processing on its behalf, the controller remains responsible for security and is required *inter alia* to choose a processor that provides sufficient guarantees in respect of the technical and organisational security measures, and must enter into a contract[348] with the processor, stipulating that the processor will act only on instructions from the controller, and that the security provisions are also incumbent on the processor.[349]

4.2.4.10 Notification to supervisory authority

The requirement of notification makes it incumbent on member states to require the data controllers, or their representatives, to furnish certain information to the supervisory authority,[350] and to require that prior checking of certain processing operations be done on the basis of this information, and that this information be published in a register of processing operations.[351]

347 Dir 95/46/EC a 17(1).

348 Or other legal act binding the processor to the controller. The parts of the contract (or other legal act) referring to data protection must be in writing (Dir 95/46/EC a 17(4)).

349 Dir 95/46/EC a 17(2) and (3).

350 See par 4.2.5.2.

351 Although the notification requirement reminds one of the registration process of the UK Data Protection Act 1984 (see Bennett *Data protection directive* 3–4), Simitis 1995 *Iowa L R* 445, 451 indicates that this provision is actually a cornerstone of the French data protection law, and was included on the insistence of the French. In the French data protection law this notification procedure is necessary because the supervisory authority has to license automated processing in most cases (Act 78–17 on Data Processing, Data Files and Individual Liberties § 16). Simitis argues that this provision looks like a "senseless exercise in bureaucracy" in the Directive, since it is not coupled with a licensing system. However, since this provision serves the transparency or openness principle, it is a good requirement (see also Battock 1995 *Int J L & Inf Tech* 156, 159). The Directive itself indicates (recitals par 48) that the notification procedure is designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national data protection legislation.

a Notification process

A data controller or its representative must notify the supervisory authority[352] before carrying out any automatic (or partly automatic) processing operation intended to serve a single purpose or several related purposes.[353] The member states may also at their discretion decide to apply the notification process to nonautomatic processing operations.[354]

The controller must at least supply the following information to the supervisory authority: the name and address of the controller and those of its representative, the purpose or purposes of the processing, a description of the category or categories of data subjects and of the data or categories of data relating to them, the recipients[355] or categories of recipients to whom the data may be disclosed, proposed transfers of data to third countries, and a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing.[356]

The notification process may be simplified or exempted by individual member states in a few cases only. This applies firstly to categories of processing operations which, taking into account the data to be processed, are unlikely to adversely affect the rights and freedoms of data subjects.[357] Certain minimum

352 See Dir 95/46/EC a 28 and par 4.2.5.2 hereunder.

353 Dir 95/46/EC a 18(1). Member states must also specify the procedures for notifying the supervisory authority of any changes in the information conveyed to them (Dir 95/46/EC a 19(2)).

354 Dir 95/46/EC a 18(5). However, member states may also decide to prescribe a simplified procedure in the case of nonautomatic processing operations.

355 "Recipient" is defined in Dir 95/46/EC a 2(g) as "a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients...".
A recipient may thus include a third party, but is not only a third party. The data subject, controller or processor all qualify as recipients.
A "third party" is defined by a 2(f) as "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data".

356 Dir 95/46/EC a 19.

357 Dir 95/46/EC a 18(2).

information must still, however, be supplied.[358]

Another instance where notification may be simplified or exempted is where the controller, in compliance with its national law, appoints a personal data protection official who is responsible for ensuring, in an independent manner, the internal application of the national provisions taken pursuant to the Directive, and who is responsible for keeping the register of processing operations carried out by the controller. This data protection official then ensures that the rights and freedoms of the data subjects are unlikely to be affected by the processing operations.[359]

The notification procedure may also be simplified or exempted in the case of nonautomatic processing operations;[360] for processing activities of which the purpose is to produce a register intended to supply information to the public;[361] or in the case of processing activities by non-profit-seeking bodies, on condition that the processing relates to the members of the body, and that the data are not disclosed to a third party without the consent of the data subjects.[362]

b Prior checking

The notification process enables the supervisory authority to carry out prior checks on processing operations likely to present specific risks to the rights and freedoms of data subjects.[363] Processing

358 Where the simplified notification procedure applies, it is sufficient if the following information is specified: the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subjects, the recipients or categories of recipients to whom the data are to be disclosed and the length of time the data are to be stored (Dir 95/46/EC a 18(2)).

359 Dir 95/46/EC a 18(2).

360 Dir 95/46/EC a 18(5). Data controllers who are released from the notification requirement must still comply with all the other requirements of their national legislation (Dir 95/46/EC recitals par (51); Battock 1995 *Int J L & Inf Tech* 156, 159).

361 Dir 95/46/EC a 18(3).

362 Dir 95/46/EC a 18(4).

363 Dir 95/46/EC a 20(1).

operations might pose such specific risks by virtue of their nature, their scope or their purpose, such as that of excluding individuals from a right, benefit or contract, or by virtue of the specific use of new technologies.[364] Member states may specify such risks in their legislation. Prior checks must be carried out by either the supervisory authority or the data protection official in cooperation with the authority.[365] Prior checks may also be carried out in the context of preparation of national legislation.[366]

c Publicising of processing operations

The supervisory authority in a member state must keep a register of processing operations about which it has been notified. The information contained in the notification sent to the supervisory authority[367] must be included in the register. The register must be open for inspection to any person.[368] Where the processing is not subject to notification, the controller or another body appointed by the member state must make the relevant information available on request.[369]

4.2.5 Implementation at national level: enforcement of principles

The Directive does not prescribe in any detail the regulatory scheme to be followed[370] by the member states. However, general rules are laid down as regards sanctions, remedies and liability, as well as the establishment of an independent supervisory authority and the drawing up of codes of conduct. In other

364 Dir 95/46/EC recitals par (53).

365 Dir 95/46/EC a 20(2).

366 Dir 95/46/EC a 20(3).

367 Except for the "general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing" (Dir 95/46/EC a 21(2)).

368 Dir 95/46/EC a 21(2).

369 Member states may provide that this provision does not apply to processing where the sole purpose is the keeping of a register, which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who has a legitimate interest (Dir 95/46/EC a 21(3)).

370 Eg, whether licensing, registration etc is required.

words, the Directive requires both a data protection authority with the necessary powers to supervise compliance with the basic data protection principles, and individual rights of enforcement independent of that authority.[371]

4.2.5.1 Judicial remedies, liability and sanctions

Individuals must be entitled to a judicial remedy, in addition to any administrative remedy,[372] for an infringement of the rights guaranteed by the national law applicable to the processing.[373] They must also be entitled to receive compensation from the controller for damage suffered as a result of an unlawful processing operation or of any act incompatible with such laws.[374] Controllers may be exempted from this liability, in whole or in part, if they prove that they are not responsible for the event giving rise to the damage.[375] The national data protection legislation must also lay down the sanctions to be imposed in the event of any infringement of its provisions.[376]

4.2.5.2 Independent supervisory authority

Each member state must establish one or more independent public authorities to monitor the application of the data protection provisions adopted pursuant to the Directive.[377] These supervisory authorities must

371 See Greenleaf 1995 (2) *Int Priv Bul* 14.

372 Eg, to the supervisory authority.

373 Dir 95/46/EC a 22.

374 Dir 95/46/EC a 23(1). According to Swire & Litan*None of your business* 42, this provision of the Directive is "stricter than any current national rules". At the time of their research in 1998, there was no member state that had an express provision in law "approving this sort of remedy for the individual".

375 Dir 95/46/EC a 23(2). Examples of situations where the controller may be exempted, are where the data subject was at fault, or in the case of *force majeure* (Dir 95/46/EC recitals par (55)).

376 Dir 95/46/EC a 24.The sanctions could be governed by either public or private law (Dir 95/46/EC recitals par (55)).

377 Dir 95/46/EC a 28(1).

be consulted when administrative measures or regulations on data protection are drawn up.[378] The authorities must be endowed with the following powers:

- investigative powers (for example, the power to access data and the power to collect all the information necessary for the performance of their supervisory duties)

- effective powers of intervention (for example, the power to deliver opinions after a prior checking has taken place;[379] to order the blocking, erasure or destruction of data; to impose a ban on processing; to warn or admonish the controller; or to refer the matter to parliament or another political institution)

- the power to engage in legal proceedings where the national data protection legislation has been violated[380]

The data subject must have the right to appeal to the courts against a decision by the supervisory body.[381]

The functions of a supervisory body should include hearing any person's claim, and informing the person of the outcome of that claim, concerning the protection of that person's rights and freedoms in regard to the processing of personal data,[382] as well as hearing claims, particularly with regard to checks on the lawfulness of data processing and informing the person that such a check has taken place.[383]

A further task of the supervisory authority is to draw up a report on its activities at regular intervals. The

---

378 Dir 95/46/EC a 28(2).

379 See par 4.2.4.10.

380 Dir 95/46/EC a 28(3).

381 Dir 95/46/EC a 28(3).

382 Dir 95/46/EC a 28(3).

383 Dir 95/46/EC a 28(4).

report must be made public.[384]

A duty of professional secrecy must be imposed on members and staff of the supervisory authority, even after their employment has ended, with regard to the confidential information to which they have access.[385]

Each member state's supervisory authority is competent to exercise the powers conferred on it within the member state's territory, even though a different national law may apply.[386] The authority of one member state may approach that of another with a request to apply its powers. The supervisory bodies are instructed to cooperate generally with one another, to the extent necessary for the performance of their duties, in particular by exchanging all useful information.[387]

4.2.5.3 Codes of conduct

Member states are to encourage the drawing up of codes of conduct for the various sectors that process data, with a view to contributing to the proper implementation of the national data protection provisions.[388] The supervisory authority of the member state must have the authority to inspect draft codes drawn up by trade associations or other representative bodies and to establish whether the codes are in accordance with national legislation.[389] It is also envisaged that codes could be developed at Community level. Such codes are to be submitted to the Working Party which gives advice on the

384 Dir 95/46/EC a 28(5).

385 Dir 95/46/EC a 28(7).

386 See par 4.2.6 on jurisdiction.

387 Dir 95/46/EC a 28(6).

388 Dir 95/46/EC a 27(1). The Directive also envisages the drawing up of codes of conduct at community level (Dir 95/46/EC a 27(3)).

389 Dir 95/46/EC a 27 (2).

implementation of the Directive.[390]

4.2.6 Jurisdiction: extraterritorial reach of national laws

Article 4 of the Directive provides that a member state's national law is applicable to the processing of data where the processing is done by a controller established[391] on the territory of the member state,[392] or where the controller is established in a place where its national law applies because of international public law,[393] or because the controller uses equipment situated on the territory of the member state (provided the equipment is not used merely for purposes of transit through the territory of the Community).[394]

In other words, a company which carries on activities in a European Union member state, but processes personal data relating to that activity in a nonmember state, will still be subject to the member state's data protection law. Likewise, a company based in a nonmember state, that uses processing facilities in a member state, will also be subject to the member state's data protection law.[395]

Bygrave[396] points to the following factors that complicate the making of rules governing the territorial reach of national data protection laws and concomitant jurisdictional and choice-of -law problems:

---

390 Dir 95/46/EC a 27 (3) and a 29. See also par 4.2.8.3.

391 "Established on the territory" of a member state implies "the effective and real exercise of activity through stable arrangements" (see Dir 95/46/EC recitals par (19)). According to this recital, the legal form of the establishment, ie whether it is merely a branch or a subsidiary with legal personality, is not the determining factor.

392 Dir 95/46/EC a 4(1)(a). When the same controller is established on the territory of several member states, it must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the applicable national law (see Dir 95/46/EC recitals par (19)).

393 Dir 95/46/EC a 4(1)(b).

394 Dir 95/46/EC a 4(1)(c). In these circumstances, the controller must designate a representative established in the territory of that member state, without prejudice to legal actions which could be initiated against the controller himself.

395 See Greenleaf 1995 (2) *Int Priv Bul* 14.

396 Bygrave 2000 *Computer L & Sec Rep* 252.

❒ the nature of data protection law in relation to private international law

Data protection law straddles the boundaries between public and private law, criminal and civil law. It is accordingly difficult to place data protection law within any one of the legal categories traditionally employed by the doctrines of private international law.

❒ the nature of the information systems that data protection law seeks to regulate

The doctrines of private international law tend to rely on an ability to establish a link to a geographical location. However, many information systems are increasingly difficult to link to any fixed geographical location. Furthermore, the doctrines of private international law tend to presume that persons and organisations are able to identify the full parameters of the informational transactions surrounding and/or affecting them. However, this ability is being challenged by the increasing complexity of informational transactions.

Article 4 is the first and only set of rules in an international data protection instrument to deal specifically with the determination of applicable law.[397] Under article 4 the principal criterion for determining applicable law is the data controller's place of establishment, largely irrespective of where the data processing occurs. This criterion will therefore become the norm for countries governed hy the Directive.[398]

4.2.7 Transfer of data to third countries

397 Bygrave 2000 *Computer L & Sec Rep* 252, 253. Bygrave points out that the drafters of the 1980 OECD Guidelines were unable to reach agreement on appropriate rules, despite discussing inter-legal issues extensively (also see par 2.2.9). The same problems appear to have been experienced by the drafters of the 1981 Council of Europe Convention (also see par 3.2.7).

398 Bygrave 2000 *Computer L & Sec Rep* 252. Bygrave also discusses problematic aspects of a 4. One of them is the possibility of "regulatory overreaching in an online environment". See further Bygrave 2000 *Computer L & Sec Rep* 252, 254–255.

An important provision in the Directive for countries outside the European Community is article 25,[399] which prescribes that member states must prohibit the transfer of personal data to nonmember countries that do not ensure an adequate[400] level of data protection.[401] All the circumstances surrounding the data transfer must be taken into account when assessing the adequacy of the level of protection afforded by a third country.[402] Factors that must be given particular consideration are the nature of the data,[403] the

399 Dir 95/46/EC a 25(1) provides:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

For Swire & Litan*None of your business* 24 the logic of a 25 is clear enough: "There would be little gained by promulgating the Directive if privacy rights are systematically violated by those handling EU citizens' personal data outside Europe." The Data Protection Working Party established by a 29 of the Directive (see par 4.2.8.3) brought out a working document in 1998 in which the practical implications of the article under discussion are looked at (see Data Protection Working Party*Transfers of personal data to third countries)*.

400 A significant part of the debate on the Directive has been over the "adequacy" provision in a 25. As Cate 1995 *Iowa L R* 431, 437 points out, while most European countries have afforded detailed protection to individual privacy rights, especially in the context of electronically stored and processed information, the United States and many other countries do not have comparable systems of data protection. Cate (438) highlights the fear American businesses with operations in Europe have that they will not be able to move personal data collected, processed or stored in Europe to the USA, even though they "own" such data. Given the importance of information in the American and global economy, this concern is understandable. Also see Swire & Litan*None of your business* 4; Estadella-Yuste 1992 *Int & Comp L Q* 170, 176; Pearce & Platten 1999 *Fordham Int LJ* 2024. On the USA and the adequacy debate, see also ch 2 par 5.

European commentators, on the other hand, have criticised the "adequacy" standard on the basis that it sets a more lenient standard for countries outside the European Community than for European Community member countries, in that it requires an "equivalent" level of data protection when personal data are transferred between two member countries (see fn 232), but only an "adequate" level of protection when personal data are transferred outside the European Community (see Schwartz 1995 *Iowa L R* 471, 483). Also see Greenleaf 1995 (2) *Int Priv Bul* 16–20.

401 The Directive makes it mandatory for member countries to prevent the transfer of data to a third country without adequate protection. This is in contrast to the OECD Guidelines (see par 2.2.7) and the Council of Europe Convention (see par 3.2.8) who do not require their signatory states to impose transborder data flow restrictions (Greenleaf 1995 (2) *Int Priv Bul* 16). Greenleaf (16) also points out that the Directive is ambiguous as to whether member countries are obliged to allow the transfer of data to third countries that do have an adequate level of protection.

In this regard it is also important to establish whether a 25 of the Directive sets minimum or maximum standards. If a 25 only sets a minimum level of protection, member countries may themselves set higher standards and thus also require a higher level of protection from other countries when personal data are transferred to such other countries. Schwartz 1995 *Iowa L R* 471 is of the opinion that a 25 sets minimum standards, because of the wording of the article, namely that "the transfer to a third country of personal data ... may take place only if ...[in compliance] with the national provisions adopted pursuant to the other provisions of this Directive". As regards the standard set in the Directive as a whole, see fn 233.

402 A 25 envisages a case-by-case approach of individual transfers. However, considering the huge number

(continued...)

purpose and duration of the proposed processing operation or operations,[404] the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules[405] and security measures which are complied with in that country.[406]

Member states and the Commission must inform each other of cases where, in their opinion, a third country does not ensure an adequate level of protection.[407] Where the Commission finds[408] that this is the case, member states must prevent any transfer of data of the same type to the country in question.[409]

402(...continued)
of transfers of personal data to third countries, this would be impossible in practice. The Working Party foresees that rationalisation will have to take place in this regard, eg by making a list of countries that are deemed in general to have an adequate level of data protection (Data Protection Working Party *Transfers of personal data to third countries* 26 (see fn 399)). Lists of this type are referred to as "white lists" (Pearce & Platten 1999 *Fordham Int LJ* 2024, 2033). Recently, the EU has ruled that Switzerland and Hungary provide adequate protection (EPIC *Privacy and human rights* 15).

403 The implication being that there will be some data that are more sensitive than others and will require a more "adequate regime" than others (Jay & Hamilton *Data protection* 110).

404 Ie, not only the nature of the data must be considered, but also the nature of the processing operations (Jay & Hamilton *Data protection* 111).

405 European commentators are critical of the use of "professional rules" as a method of regulating data protection. They argue that such rules cannot be considered apart from the legislative provisions of the third country in question, because it is difficult to establish the content of such rules, they are subject to unilateral change, and they can be used as a smoke screen (Schwartz 1995 *Iowa L R* 471, 485–486).

406 See Schwartz & Reidenberg *Data privacy law* for an example of how such an evaluation could be done. These two American law professors were asked by the European Commission to conduct a study of US data protection law, to determine the extent to which the processing operations in the US are guided by the same principles as those acknowledged in the Directive (see Schwartz & Reidenberg *Data privacy law* ix). To do this, the authors looked at the US Constitution and state constitutions, federal and state legislation, federal and state court decisions, practices by administrative bodies in both the public and the private sector, practices by self-regulating bodies, industry and company codes of practice, and the policies of American corporations (Schwartz & Reidenberg *Data privacy law* 6–12). The EU and the USA have since adopted the "Safe Harbor" agreement (for more on this, see ch 2 par 5).

407 Dir 95/46/EC a 25(3).

408 The Commission is assisted in this regard by a committee, composed of representatives of the member states and chaired by the representative of the Commission (see Dir 95/46/EC a 31).

409 Dir 95/46/EC a 25(4). This provision obliges member states to cut off the flow of personal information to a third country, and therefore has potentially grave consequences for countries outside the European union (see Schwartz 1995 *Iowa L R* 471, 487). Schwartz refers to this kind of prohibition as a "data embargo order". Many of the European data protection authorities have such an administrative power in terms of their
(continued...)

The Commission is instructed to enter into negotiations with third countries that fall short on the adequacy provision, at the appropriate time, to remedy the situation.[410] Upon conclusion of such negotiations, the Commission may find[411] that the third country does ensure an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. In such an instance, member states must take the measures necessary to comply with the Commission's decision.[412]

In article 26 the Directive provides for derogations from the prohibition of transfer of data to third countries without adequate protection for privacy in the following circumstances:[413]

- The data subject has unambiguously consented to the proposed transfer.[414] The consent must be freely given, specific and informed.[415] This implies that the data subject must be informed about the risk that personal data relating to the subject could be transferred to a country without adequate protection.[416] Implied consent would not satisfy this provision.

- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data

409(...continued)
national legislation. He distinguishes (488–489) between a preventive data embargo that seeks to prevent harm, and a structural order that restructures or alters a planned data transfer to bring it into conformity with the demands of domestic data protection law. An order combining these two elements is also possible.

410 Dir 95/46/EC a 25(5).

411 In accordance with a procedure provided for in Dir 95/46/EC a 31(2). See fn 408.

412 Dir 95/46/EC a 25(6).

413 These exemptions concern cases where the risks to the data subject are relatively small or where other interests (public interests or those of the data subject himself) override the data subject's right to privacy (Data Protection Working Party *Transfers of personal data to third countries* 24).

414 Dir 95/46/EC a 26(1)(a). Swire & Litan *None of your business* 34 point out three limitations to this exception: First, the past tense "has given" suggests that the consent must be given before the transfer; second the consent must be given unambiguously; and third the consent to the proposed transfer actually requires consent to the particular uses to which the data will be put.

415 See the definition of "data subject's consent" in a 2(h) (quoted in fn 271).

416 See Data Protection Working Party *Transfers of personal data to third countries* 24.

subject's request.[417]

- ❒ The transfer is necessary for the conclusion or performance of a contract, concluded in the interest of the data subject, between the controller and a third party.[418]

- ❒ The transfer is necessary or legally required on important public interest grounds,[419] or for the establishment, exercise or defence of legal claims.[420]

- ❒ The transfer is necessary in order to protect the vital interests of the data subject.[421]

- ❒ The transfer has been made from a register established by law and intended for consultation by the public or persons having a legitimate interest.[422]

---

417 Dir 95/46/EC a 26(1)(b).

418 Dir 95/46/EC a 26(1)(c). Examples of transfers where the exemptions in a 26(1)(b) and a 26(1)(c) will apply, are when transfers are made to reserve an airline ticket for a passenger or to effect an international credit card payment. An example of the situation where the contract is for the benefit of the data subject would be where the data subject is the beneficiary of a payment made by the third party to the controller. A "necessity test" must be applied in these cases: all of the data transferred must be **necessary** for the performance of the contract. If additional nonessential data are transferred, or if the purpose of the transfer is not the performance of a contract but some other purpose (eg follow-up marketing), the exemption will be lost. See Data Protection Working Party *Transfers of personal data to third countries* 24. Also see Swire & Litan *None of your business* 34–35.

419 Examples of situations where transfer of data may be allowed on important public interest grounds are in cases of international transfers of data between tax or customs administrations or between services competent for social security matters (Dir 95/46/EC recitals par (58)).

420 Dir 95/46/EC a 26(1)(d). These transfers must obviously take place in the context of international litigation or legal proceedings (Data Protection Working Party *Transfers of personal data to third countries* 25).

421 An example of such a transfer is where medical data need to be urgently transferred to a third country from a member country where the data subject has previously been treated, because the data subject has become seriously ill while visiting the third country. "Vital interest" must be interpreted narrowly, however, and must not include financial, property or family interests. See Data Protection Working Party *Transfers of personal data to third countries* 25.

422 Dir 95/46/EC a 26(1)(f). In such a case the transfer must not involve the entirety of the data or entire categories of the data contained in the register. Where the register is intended for persons with a legitimate interest, the transfer must only be made at the request of those persons, or if they are to be recipients (Dir 95/46/EC recitals par (58)).The intention of this exemption is that where a register in a member state is

(continued...)

❒ Where the controller provides adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals. This might be done by means of appropriate contractual clauses.[423] When permission is granted on this ground, the member state must inform the Commission and the other member states.[424]

If the Commission or other member states object on justifiable grounds that relate to the protection of the privacy and fundamental rights and freedoms of individuals, the Commission must take appropriate measures,[425] with which the member states must comply.[426] On the other hand, should the Commission decide[427] that the standard contractual clauses offer sufficient safeguards, member states must take the

422(...continued)
available for consultation by the public or persons demonstrating a legitimate interest, then the fact that the person who has the right to consult the register is situated in a third country, and that the act of consultation would therefore involve a transfer of data, must not prevent the information being transmitted to such a person. See Data Protection Working Party *Transfers of personal data to third countries* 25.

423 Dir 95/46/EC a 26(2). The so-called "contractual solution" to the problem of inadequate data protection. Schwartz 1995 *Iowa L R* 471, 491 explains the contractual solution:

> A contractual solution refers to a written agreement between the data exporter and the data importer. The domestic data protection authority oversees the drafting of an agreement to arrive at a negotiated solution to an otherwise problematic international data transfer. In such a contract, the importer promises to provide additional measures of data protection.

European experts are sceptical about the use of contracts to regulate data protection. Schwartz 1995 *Iowa L R* 471, 492 points out the weaknesses of such an arrangement:

> First, a domestic data protection authority lacks the power to enforce such agreements once the personal data leaves the land of its origin....Thus, contractual solutions will, at best, be fated to under-enforcement.... Finally, ... a contract may rely excessively upon a company's "code of conduct," or other written policy defining internal practices regarding data protection. These policies have some potential to improve data protection in the private sector. But, since these business practices are subject to unilateral change, they cannot be seen as commensurate with a foreign nation's statutory data protection law.

Also see Walden "Data protection" 451. The English law doctrine of privity of contract also presents problems regarding the use of contracts to secure rights for third parties in the UK (Jay & Hamilton *Data protection* 119). Also see ch 4 par 4.3.4.9. The Data Protection Working Party has taken a more positive view of the role of contractual provisions in providing adequate data protection (Data Protection Working Party *Transfers of personal data to third countries* 15 *et seq*). Also see Heydrich 1999 *Brooklyn J Int L* 407.

424 Dir 95/46/EC a 26(3). This provision aims to provide a safeguard against the contractual solution (see fn 423), in the light of the criticism thereof.

425 In accordance with a procedure provided for in article 31(2). See fn 408.

426 Dir 95/46/EC a 26(3).

427 In accordance with a procedure provided for in article 31(2). See fn 408 and accompanying text.

necessary measures to comply with the Commission's decision.[428]

The Data Protection Working Party has provided guidance on the interpretation of articles 25 and 26.[429] According to the Working Party, any meaningful analysis of "adequate protection" must comprise two elements: an assessment of the content of the rules applicable and an assessment of the means of ensuring their effective application. The Working Party suggests that a core of data protection content principles and procedural enforcement requirements can be identified, compliance with which could be seen as a minimum requirement for protection to be considered adequate.[430]

Those principles and requirements are as follows: [431]

Content principles

- the purpose limitation principle

  Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in article 13 of the Directive.

- the data quality and proportionality principle

  Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further

428 Dir 95/46/EC a 26(4).

429 Data Protection Working Party *Transfers of personal data to third countries* (see fn 399).

430 Data Protection Working Party *Transfers of personal data to third countries* 5.

431 Data Protection Working Party *Transfers of personal data to third countries* 6–7.

processed.

- the transparency principle

  Individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with articles 11(2) and 13 of the Directive.

- the security principle

  The data controller should take the technical and organisational security measures that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except when instructed to do so by the controller.

- the rights of access, rectification and opposition

  The data subject should have a right to obtain a copy of all data relating to him or her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he or she should also be able to object to the processing of the data relating to him or her. The only exceptions to these rights should be in line with article 13 of the Directive.

- restrictions on onward transfers

  Further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (that is the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should

be in line with article 26(1) of the Directive.

Examples of additional principles to be applied to specific types of processing are:

- sensitive data

  Where sensitive categories of data are involved (those listed in article 8 of the Directive), additional safeguards should be in place, such as a requirement that the data subject gives his or her explicit consent for the processing.

- direct marketing

  Where data are transferred for the purposes of direct marketing, the data subject should be able to opt-out from having his or her data used for such purposes at any stage.

- automated individual decision

  Where the purpose of the transfer is the taking of an automated decision in the sense of article 15 of the Directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interests.

Procedural or enforcement mechanisms

According to the Working Party, although there is broad agreement in Europe that data protection principles should be embodied in law and that a system of external supervision in the form of an independent authority is a necessary feature of a data protection compliance system, these features are not always present elsewhere in the world. To provide a basis for the assessment of the adequacy of the protection provided, it is therefore necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural

mechanisms used in third countries.

According to the Working Party the objectives of a data protection system are essentially threefold:

- to deliver a good level of compliance with the rules

  A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important part in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

- to provide support and help to individual data subjects in the exercise of their rights

  The individual must be able to enforce his or her rights rapidly and effectively, and without prohibitive cost – some sort of institutional mechanism allowing independent investigation of complaints is therefore necessary

- to provide appropriate redress to the injured party where rules are not complied with

  This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

According to Aldhouse,[432] although the impression may be created that the Working Party requires every third country to have an omnibus data protection law, that is not the case. The Working Party also recognises that adequate protection can be delivered by self-regulation,[433] and that contractual arrangements can both provide adequate alternative safeguards and form part of the package of self-

432 Aldhouse 1999 *Int R L Computers & Tech* 75, 77.

433 Data Protection Working Party *Transfers of personal data to third countries* 10–14.

regulation to provide adequacy.[434]

4.2.8 Supervision of Directive at European Union level

Supervision of the Directive is distributed between the Commission of the European Union (EU), a Committee of Representatives of EU member states (and in some instances the EU Council itself), and an advisory Working Party drawn from the national data protection authorities.[435]

4.2.8.1 EU Commission

The Commission is to report to the Council and the European Parliament at regular intervals on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report is to be made public. The Commission must also examine the application of the Directive to the data processing of sound and image data, and submit proposals in this regard.[436]

The Commission must furthermore advise the Working Party of the action it has taken in response to its opinions and recommendations,[437] and must negotiate with nonmember states concerning the "adequate protection" requirement of article 25.[438]

4.2.8.2 Committee of member states and EU Council

The Directive provides for the establishment of a Committee composed of the representatives of the member states and chaired by the representative of the Commission. The Committee must assist the

434 Data Protection Working Party *Transfers of personal data to third countries* 15–22.

435 See Greenleaf 1995 (2) *Int Priv Bul* 15.

436 Dir 95/46/EC a 33.

437 Dir 95/46/EC a 30(5).

438 Dir 95/46/EC a 25(5).

Commission.[439]

The Commission is to submit to the Committee a draft proposal containg the implementing measures it recommends should be taken by the Community,[440] and the Committee must deliver its opinion on the draft within a time limit which the chairperson may lay down, depending on the urgency of the matter.[441]

If the Committee approves the proposed measures, the Commission must adopt them. If they are not approved, the proposed measures should be referred to the Council of Ministers.[442]

4.2.8.3 Working Party

In article 29, the Directive sets up an independent Working Party on the Protection of Individuals with regard to the Processing of Personal Data, with advisory status.[443] The Working Party is composed of representatives of the supervisory authority of each member state, representatives of the authority established for the Community institutions and bodies, and representatives of the Commission.[444] The Working Party elects its own chairperson,[445] adopts its own rules of procedure[446] and takes decisions by a simple majority of the representatives of the supervisory authorities.[447] Its secretariat is provided

439 Dir 95/46/EC a 31(1).

440 This includes decisions on adequacy of third countries' laws and proposed authorisations of data transfers (Greenleaf 1995 (2) *Int Priv Bul* 15).

441 Dir 95/46/EC a 31(2).

442 Dir 95/46/EC a 31(2)

443 Dir 95/46/EC a 29(1).

444 Dir 95/46/EC a 29(2).

445 Dir 95/46/EC a 29(4). The chairperson's term of office is two years, and he or she is eligible for reelection. The first chairperson elected was Peter Hustinx from the Netherlands Data Protection Authority.

446 Dir 95/46/EC a 29(6).

447 Dir 95/46/EC a 29(3).

by the Commission.[448] Items to be considered by the Working Party are placed on its agenda by its chairperson, either on his or her own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.[449]

In general it can be said that the function of the Working Party is to advise the Commission and to contribute to the uniform application of the national rules adopted pursuant to the Directive.[450] In more precise terms, the Working Party must examine any question regarding the application of the national measures adopted pursuant to the Directive, in order to contribute to the uniform application of such measures; give the Commission an opinion on the level of protection in the Community and in third countries; advise the Commission on any proposed amendment of the Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons, with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms; and give an opinion on codes of conduct drawn up at Community level.[451]

The Working Party must inform the Commission if it finds that divergences are arising between the data protection provisions of member states where such divergences are likely to affect the equivalence of protection in the different member states.[452] The Working Party may also on its own initiative, make recommendations on data protection issues to the Commission.[453] The Commission must, in a public report, inform the Working Party, the European Parliament and the Council of the action it has taken in response to the Working Party's recommendations.[454]

448 Dir 95/46/EC a 29(5).

449 Dir 95/46/EC a 29(7).

450 Dir 95/46/EC recitals par (65). Schwartz 1995 *Iowa L R* 471, 483 describes the Working Party as "a new institution of data protection oversight on the Europe-wide level".

451 Dir 95/46/EC a 30.

452 Dir 95/46/EC a 30(2).

453 Assisted by the committee (see fn 408 and Dir 95/46/EC a 30(4)).

454 Dir 95/46/EC a 30(5).

The Working Party must annually draw up a report on the situation regarding the protection of natural persons, with regard to the processing of personal data in the Community and in third countries.[455] The Working Party must transmit the report, which must be made public, to the Commission, the European Parliament and the Council.[456]

4.2.9 Freedom of information

The Directive does not have specific provisions on freedom of information, but states that it allows the principle of public access to official documents to be taken into account when implementing the principles set out in the Directive.[457]

4.3 Conclusion

The adoption of the Directive was followed by a period in which European Union member countries had to redraft their existing legislation to meet the requirements of the Directive.[458] For nonmember countries there will be a time of speculation on what the provisions in the Directive actually mean for them, and on whether those provisions will, or can, be enforced in "an increasingly complex, distributed, and interconnected computing environment".[459]

---

455 Reports have been submitted annually since 1997, eg Data Protection Working Party *First annual report* (1997); *Second annual report* (1998); *Third annual report* (1999).

456 Dir 95/46/EC a 30(6). The Commission must examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and must submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and the state of progress in the information society (Dir 95/46/EC a 33).

457 Dir 95/46/EC recitals par (72). For a discussion of this issue, see Maxeiner 1995 *Fed Comm LJ* 93.

458 Countries such as Greece and Italy, which did not have data protection legislation in 1995, had the opportunity to draft such legislation for the first time. By mid 1998 Austria, Belgium, Denmark, Spain, Germany, France, Ireland, Luxembourg, the Netherlands, Portugal, Finland, Sweden, and the UK had all embarked on a process of transposing the Directive into their national laws (Data Protection Working Party *Second annual report* 5–7).

459 Bennett & Raab 1997 *Inf Soc* 245, 246. Swire & Litan *None of your business* 50–51 are of the opinion that the Directive is designed for the regulation of mainframe computers and are therefore more likely to be enforceable in that context. They argue that the Directive appears to be less suited to solve privacy

(continued...)

The Directive suffers from some major drawbacks: it is very complicated, a fact that will detract from its value as an instrument that individuals might cite and use; many of the provisions can be interpreted in different ways, because its meaning is concealed in complicated wording or within lengthy recitals; and the different time limits for implementation also add to its incoherence.[460]

However, it has also been responsible for some real innovations in data protection policy: it abandons artificial and outdated distinctions such as that between the public and private sector, between "automated" and "manual" files,[461] and between the different stages of processing.[462]

Whether the purpose of the Directive, namely to harmonise European data protection policy at a high level of protection[463] will be met, depends a lot on subsequent interpretation and implementation by the European Union member countries.[464] Nevertheless, for most commentators, the Directive represents "the most modern international consensus on the desirable content of data protection rights and may be a valuable model for countries currently without data protection laws".[465] The importance of the Directive is emphasised by Swire and Litan[466] in the following words:

> The EU Directive represents a dramatic increase in the reach and importance of data protection laws. Once it goes into effect in October 1998, a unified and comprehensive data protection regime will apply to all fifteen countries and 370 million people in the

459(...continued)
problems in distributed (network) processing. The language of the Directive, eg terms such as "controller" and "data subject" is apt in the mainframe environment, but far less apt in a world of personal computers and the Internet.

460 Bennett & Raab 1997 *Inf Soc* 245, 252.

461 See par 4.2.3.

462 See fn 238.

463 See par 4.2.2.

464 Bennett & Raab 1997 *Inf Soc* 245, 253.

465 Greenleaf 1995 (2) *Int Priv Bul* 1; Cate *Information age* 45.

466 Swire & Litan *None of your business* 24.

European Union.

4.4 EU initiatives following the Directive

Two more Directives that have implications for data protection have been adopted since the 1995 Directive on data protection, namely the Directive concerning the Protection of Personal Data and the Protection of Privacy in the Telecommunications Sector, (the Directive concerning privacy and telecommunications) in 1997,[467] and the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (the Directive on privacy and electronic communications) in 2002.

The Directive concerning privacy and telecommunications establishes specific protections for telephone, digital television, mobile networks and other telecommunications systems. It imposes wide-ranging obligations on carriers and service providers to ensure the privacy of users' communications, including that of users of the Internet. Access to billing data is severely restricted. It also restricts direct marketing activities. Caller identification technology is required to incorporate an option for per-line blocking of number transmission. Information that is collected in the delivery of a communication must be purged once the call has been completed.[468]

The Directive on privacy and electronic communications was first proposed in July 2000. In the form originally proposed, this Directive would have reinforced privacy rights for individuals by extending the protective measures that were already in place for telecommunications to a broader, more technology-neutral category of "electronic communications". EPIC[469] reports that during the process, however, the Council of Ministers began to push for the inclusion of data retention provisions, requiring

467 Directive 97/66/EC (1998 *Official Journal* L 24/1). Sometimes this Directive is referred to as the ISDN Directive as it partially relates to the Integrated Services Digital Network and digital mobile networks (Singleton *Data protection* 79). The date for its implementation was exactly the same as that for the data protection Directive, ie 24 October 1998.

468 See also EPIC *Privacy and human rights* 11.

469 EPIC *Privacy and human rights* 11.

Internet Service Providers and telecommunications operators to store logs of all telephone calls, e-mails, faxes, and Internet activity for law enforcement purposes. These proposals were strongly opposed by most of the members of the Parliament. However, following the events of 11 September 2001 the political climate changed and the Parliament came under increasing pressure from member states to adopt the Council's proposal for data retention. The United Kingdom and the Netherlands, in particular, questioned whether the proposed privacy rules still struck the right balance between privacy and the needs of the law enforcement agencies in the light of the battle against terrorism. On 25 June 2002 the European Union Council adopted the new Directive on privacy and electronic communications[470] in terms of which member states may now pass laws mandating the retention of the traffic and location data of all communications taking place over mobile phones, SMS, landline telephones, faxes, e-mails, chatrooms, the Internet, or any other electronic communication device. Such requirements can be implemented for purposes varying from national security to the prevention and investigation of criminal offences and the prosecution of offenders.[471]

The Directive on privacy and electronic communications also has positive aspects from a privacy perspective. For example, the consumer's right to privacy and control over personal data are enhanced in relation to "calls", "communications", "traffic data" and "location data". These new provisions ensure the protection of all information ("traffic") transmitted across the Internet, prohibit unsolicited commercial marketing by e-mail (so-called "spam")[472] without consent, and protect mobile phone users from precise location tracking and surveillance. The Directive also gives subscribers to all electronic communications services (such as GSM and e-mail) the right to choose whether they want to be listed in a public directory.[473]

470 *Official Journal* L 201 (31 July 2002).

471 EPIC *Privacy and human rights* 12.

472 See ch 1 par 1.3.

473 EPIC *Privacy and human rights* 23–13.