Chapter 6
Comparative law conclusions

Contents

1 INTRODUCTION – NECESSITY OF DATA PROTECTION LEGISLATION

1.1 General protection

In all the countries studied, the problem of invasion of privacy through the misuse of personal information was brought to the fore by the same technological development, namely the computer.[1] Before the advent of the computer, privacy was recognised in most of these countries[2] and personal information was collected by governments and private companies. However, the computer and the rapid development and spread of information technology through the industrialised world suddenly made it possible to collect, store and retrieve vast amounts of personal information and to manipulate this information in ways never before imagined. The threat posed by the computer and the reaction of citizens to the perceived threat to their privacy prompted the legislators in the various countries to consider legislation at about the same time.[3] This meant that countries were able to learn from each

1 Also see Bennett *Regulating privacy* 118; Mogg 1994 (Nov/Dec) *TDR* 29. However, it is important to remember that, as Hondius 1983 *Neth Int LR* 103, 104 puts it, the "computer is the catalyst, not the central issue of data protection".

2 Even in the UK where privacy is not explicitly recognised, it was protected under the guise of other legal concepts (see ch 4 par 2). On the recognition of the right to privacy in the USA, see ch 2 par 3 and in the Netherlands, see ch 5 par 3.

3 The world's first data protection act was the data protection statute of the German state of Hesse, adopted (continued...)

other in drafting their legislation.[4]

International contact and cooperation was largely responsible for the similarity displayed by data protection legislation.[5] The fact that the primary interest at stake (namely privacy[6]) deserved equal and universal protection[7] meant that the legislative measures taken to protect it would of necessity be similar.

International cooperation was strengthened through the involvement of international organisations, such as the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe. The OECD's Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[8] and the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[9] resemble one another closely, which is to be expected since they were

3(...continued)
in 1970. (This was not a national data protection act.) As seen, plans by governments to hold national censuses around 1970 in which computer technology would have been used, plans to create national data bases of personal information, coupled with alarmist "Big Brother" literature, and the efforts of privacy lobbies, brought the problem to the attention of the public in the countries studied. See ch 2 par 4.2.1; ch 5 par 4.2.1; ch 4 par 4.2.1. Also see Bygrave *Data protection law* 93 *et seq*.

4 Bennett *Regulating privacy* 124 indicates that the first national data protection act, the Swedish Data Act of 1973, was translated into eg English, French and German and delegations from many European countries visited Sweden during the Act's first years to learn more about it.

5 Hondius, an international data protection expert, summarises this situation aptly (see Hondius 1983 *Neth Int L R* 103, 104):

> Data protection has been from the outset an international matter. Information technology and its applications in data processing are used in the same way in many countries and are developed by a multinational industry. Scarcity of expertise and the desire to avoid unnecessary divergencies between national laws have created a need for frequent international consultation. Rules of international law have been introduced to make national laws more effective and to deal with the phenomenon of transborder data flows.

6 It will be shown in ch 7 that another interest, namely identity, is infringed when false information is processed. However, none of the countries studied recognised identity*eo nomine* as a separate personality interest. The interests protected by data protection are referred to as the individual's "fundamental rights and freedoms ... in particular the right to privacy" (see eg Dir 95/46/EC a 1(1)).

7 Hondius 1983 *Neth Int L R* 103, 104; Neethling *Privaatheid* 275.

8 See ch 3 par 2.

9 See ch 3 par 3.

formulated and discussed during the same period and to a large extent by the same countries.[10] The OECD in particular provided a forum for both Americans and Europeans to debate the safeguarding of privacy in the computer age.[11]

As indicated, 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[12] aims to harmonise data protection laws in the European Union, but because of its prohibition on the transfer of personal data to non-member countries that do not ensure an adequate level of data protection, it will also influence data protection legislation in non EU-countries.

The rationale for the harmonisation of data protection laws is that if all countries involved in the transfer of personal data across national boundaries provide a level of protection of the privacy of individuals that can be considered adequate by international standards, the free flow of information can be ensured.[13]

It can be concluded that data protection legislation is absolutely necessary *inter alia* to protect the privacy of individuals, who can no longer control the use made of their personal information in the light of the massive changes in information handling activities during the past few decades.[14] All modern

10 See ch 3 par 1, and see Hondius 1983 *Neth Int L R* 103, 113.

11 See Bennett *Regulating privacy* 138.

12 See ch 3 par 4.

13 This is also why international documents on data protection were thought to be necessary (see ch 3 par 1).

14 As Simitis 1985 (8) *TDR* 95 puts it:

> It has been recognised, at least since the Council of Europe Convention of 28 January 1981, that data protection is not a problem peculiar to a specific legal system, but that it is vital to the functioning of every democratic society. Fundamental rights are lost for ever if citizens neither know nor have any means of finding out who collects information about them and on what occasion this is done.

See also Flaherty *Surveillance societies* 371.

countries today either have data protection legislation in place or are in the process of enacting it.[15] Provisions in these laws to the effect that transfer of personal data may only take place to countries that provide adequate protection of personal information mean that countries without data protection legislation will have to adopt such legislation that meets international standards if they want to remain part of the international information community.[16]

1.2 Transborder protection of personal data

As has been said,[17] it had been recognised since the 1980s that data protection is an international problem. With the global market leading to an increase in the exchange of information, including personal information, across national boundaries,[18] international organisations have come to realise the necessity of harmonising data protection laws to prevent the creation of data havens which could nullify countries' efforts to protect their citizens' liberties,[19] but at the same time enable the free flow of information across national boundaries.[20] All the international documents issued since the 1980s therefore have two primary goals, namely the setting of standards at the national level for the protection of personal data and the reconciliation of this goal with the ideal of allowing the free flow of information across national boundaries.[21]

For example, while one purpose of the EU Directive is to ensure the free flow of personal data between

15 For a list of countries which had data protection laws in place at the end of 2002, see ch 1 fn 41.

16 See also text to fn 13.

17 See ch 3 par 1.

18 Referred to as "transborder data flows" (TBDF).

19 EPIC *Privacy and human rights* 14.

20 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" (Pinegar 1984 *Int Bus L'yer* 183, 187). See also McKeaver 1984 *Int Bus L'yer* 159; Schlundt 1985 *InfAge* 67, 68. There would appear to be a suspicion, especially in the USA, that Europe is using data protection legislation as a pretext for economic protectionism (Lloyd *Information technology law* 48).

21 See ch 3 par 2.2.3, par 3.2.2 and 4.2.2. Also see EPIC *Privacy and human rights* 15.

the member states of the European Community, it also represents an attempt to ensure a high level of protection for individuals' right to privacy.[22] Member states are therefore compelled to adopt legislation which conforms to the standards set in the Directive, so that "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". By coordinating the laws of the member states, the EU aims "to ensure that the cross-border flow of personal data is regulated in a consistent manner ..." The Directive also expresses the need for Community action to "approximate" data protection laws.[23] Once the objective of "equivalency" between or "harmonisation" of the data protection laws of the member states' has been reached,[24] 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.[25]

As has been pointed out,[26] there would be little to be gained by promulgating the Directive if the privacy rights of the citizens of EU countries are systematically violated by those handling their personal data outside Europe. Third countries (in other words, nonmember countries) are therefore also affected by the provisions of the Directive through article 25,[27] which provides that member states must prohibit the transfer of personal data to nonmember countries that do not ensure an adequate level of data protection.[28] Article 26 of the Directive provides for derogations from this prohibition in specific

22 See ch 3 par 4.2.2.

23 Dir 95/46/EC recitals par (8). See further ch 3 par 4.2.2.

24 Dir 95/46/EC recitals par (8). The terms "approximation" and "harmonisation" of national laws are synonymous. "Harmonisation" is a technical term of European Community law that refers to formal attempts to increase the similarity of legal measures in member nations (Schwartz 1995 *Iowa L R* 471, 481).

25 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.)

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

27 Dir 95/46/EC a 25(1).

28 A significant part of the debate on the Directive has been over the "adequacy" provision in a 25. On the USA and the adequacy debate, see also ch 2 par 5.

circumstances.[29]

The Data Protection Working Party has supplied guidance on the interpretation of articles 25 and 26.[30] 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 could be identified, compliance with which could be seen as a minimum requirement for protection to be considered adequate.[31]

It has been argued that the Working Party does not require every third country to have an omnibus data protection law in order to meet the adequate protection standard of the Directive.[32] Adequate protection can be delivered by means such as self-regulation.[33] Contractual arrangements can also form part of the package of self-regulation to provide adequacy.[34]

29 See ch 3 par 4.2.7 for a detailed discussion of Dir 95/46/EC a 25 and 26.

30 Data Protection Working Party *Transfers of data to third countries*.

31 For a detailed discussion of the Working Party's proposals, see ch 3 par 4.2.7. In brief, the "content principles" are the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, the rights of access, rectification and opposition and restrictions on onward transfers. Additional principles should be applied to the processing of sensitive data, processing for the purposes of direct marketing or for taking automated individual decisions. With regard to "procedural or enforcement mechanisms", the Working Party identified the underlying objectives of a data protection procedural system, on which basis the different judicial and non-judicial procedural mechanisms used in third countries should be judged. 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; to provide support and help to individual data subjects in the exercise of their rights and to provide appropriate redress to the injured party where rules are not complied with (see also ch 9 par 5.1).

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

33 Data Protection Working Party*Transfers of data to third countries* 10–14. On self-regulation, see par 2.5.1.3 below.

34 Data Protection Working Party *Transfers of data to third countries*15–22. On the "contractual solution" to data protection, see ch 3 par 4.2.7 and ch 4 par 4.3.4.9. See also Schwartz 1995 *Iowa L R* 471, 491; Reed & Angel *Computer law* 331; Jay & Hamilton *Data protection* 119; Heydrich 1999 *Brooklyn J of Int L* 407; Data Protection Working Party *Transfers of data to third countries* 15 *et seq*.

2 SIMILARITY IN DATA PROTECTION PRINCIPLES; DIFFERENCES IN IMPLEMENTATION

2.1 Introduction

Commentators have pointed out that, despite differences in language, legal traditions and cultural and social values, there has been a broad measure of agreement on the basic content and core rules that should be embodied in data protection legislation.[35] The areas in which data protection laws differ the most are the scope of the laws and the mechanisms employed to enforce the core data protection principles. After identifying and discussing the core data protection principles that are to be found in the laws studied, differences in the scope of the laws and the enforcement of the principles will be analysed.

2.2 Core principles of data protection law

Some of the Acts and legal instruments studied explicitly contain a set of data protection principles.[36] Examples are the OECD (Organisation for Economic Co-operation and Development) Guidelines, which embody a set of eight basic principles of data protection,[37] as does the Council of Europe Convention (the Convention)[38] and the UK Data Protection Act of 1998 (DP Act).[39] However, even those Acts or instruments that do not explicitly refer to data protection principles (such as the USA Privacy Act of 1974 and the Fair Credit Reporting Act of 1970, and the Dutch Wet Bescherming Persoonsgegevens of 2000 (WBP)) give effect to certain basic or core data protection principles. Some of these laws are more effective in doing so than others.

35 Bennett *Regulating privacy* 95; Flaherty *Surveillance societies* 379.

36 Also referred to as "fair information principles" (see eg ch 2 par 4.2.2.7; ch 4 par 4.2.1.6).

37 See ch 3 par 2.2.5.

38 Convention 108/1981 (see ch 3 par 3.2.4).

39 See ch 4 par 4.3.4.

It is submitted that the following ten core data protection principles can be identified, in one form or another,[40] in all successful data protection laws:[41]

2.2.1 Fair and lawful processing

The first principle of data protection laws is that personal data must be processed fairly and lawfully.

In the USA laws, the idea of fairness is reflected in the Privacy Act's stated purpose of striking an appropriate balance between the need of individuals for a maximum degree of privacy over the personal information they furnish to the government, and the need of the government for information about the individual which it requires in order to carry out its legitimate functions.[42] The principle of lawful processing is also reflected in the agency requirements.[43] The Fair Credit Reporting Act is aimed at promoting fairness in credit reporting, and consumer reports may only be disclosed lawfully if this is done within the confines of the Act.[44]

The principle of fair and lawful processing is reflected in the OECD Guidelines' requirement that personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.[45] It is furthermore reflected in the principles of the Council of Europe Convention which provide *inter alia* that personal data undergoing automatic processing should be

40 See Bygrave *Data protection laws* 57–69; Bennett *Regulating privacy* 101–111. Not all commentators or legal instruments have ten principles, or include all the principles exactly as formulated here. It is also not always possible to make rigid distinctions between the principles and one will find that some of them overlap to some extent.

41 Flaherty (a former Data Protection Commissioner for BC, Canada) is of the opinion that fair information practises are adequate to deal with any privacy issue, even in the next decade. After researching the field of data protection for more than thirty years and practising as a data protection commissioner, he writes that he has never met a privacy issue that could not be satisfactorily addressed by the application of fair information practices (Flaherty "Visions of privacy" 35).

42 Pub L 93–579 s 2(b) (see ch 2 par 4.2.2.2).

43 5 USC s 552a(e) (see ch 2 par 4.2.2.7).

44 15 USC s 1681b(a) (see ch 2 par 4.3.2.3).

45 OECD Guidelines par 7 (see ch 3 par 2.2.5.1).

obtained and processed fairly and lawfully.[46] The EU Directive also requires that personal data must be processed fairly and lawfully.[47]

The UK DP Act contains a set of eight general data protection principles, the first of which explicitly requires that personal data must be processed fairly and lawfully.[48] In interpreting the first principle, the Act requires fairness in processing data (the so-called fair processing code) and compliance with specific conditions in order to make processing lawful. The fair processing code involves fairness in obtaining the information, in providing the data subject with specific information, as well as fairness regarding conditions for processing personal identifiers.[49] The Data Protection Registrar has advised that fairness and lawfulness should both be tested against an objective standard in which the intentions or views of the data controller are not relevant.[50]

The Dutch WBP also requires data controllers to process personal data in accordance with the law and in a proper and careful manner (*behoorlijke en zorguldige wijze*).[51] The Dutch government did not follow the wording of the Directive which requires "fair and lawful" processing (the Dutch translation of "fair and lawful" is "*eerlijk en rechtmatig*") because it considered the phrase to be tautological: if processing is "*oneerlijk*", it is also "*onrechtmatig*" and *vice versa*. It was therefore felt that the requirement that processing should be done "*behoorlijk en zorguldig*" is a better reflection of the standard required in society to prevent an unlawful act.[52] The WBP spells out specific principles that

46 Convention 108/1981 a 5 (see ch 3 par 3.2.4.1).

47 Dir 95/46/EC a 6(1)(a) (see ch 3 par 4.2.4.1).

48 DP Act of 1998 sch 1 part 1 (see ch 4 par 4.3.4.2).

49 DP Act of 1998 sch 1 part II par 1(1).

50 DPR *Guidelines* 59 (see ch 4 par 4.3.4.2).

51 WBP a 6. This article is considered to be the "*moederartikel*" of the WBP, which incorporates the legality principle for the processing of data. The articles following on a 6, namely a 7, 8 and 9, describe what may or may not be considered to be "proper and fair" (Schreuders 1998 (2) *Priv & Inf* 52, 53–54). See further ch 5 par 4.3.4.1.

52 WBP *Memorie van toelichting* 78 (see ch 5 par 4.3.4.1).

must be complied with to ensure that processing is lawful.[53]

In English and American law the term "fair" seems to have a broader meaning than in Dutch law. For example, Bygrave, mentions that "fair" has a less obvious and potentially broader meaning than "lawful". At a general level he interprets "fair" to mean that data controllers must take account of the interests and reasonable expectations of data subjects.[54]

Bygrave[55] points out that the principle of fair and lawful processing is primary because "it embraces and generates the other core principles of data protection laws". Stated differently, if all the other data processing principles are applied, the result will be that processing is done fairly and lawfully. In the South African context, however, it sufficient to require that processing should be done lawfully, since fairness is part and parcel of the concept of lawfulness.[56]

It is submitted that the ultimate aim of any data protection law should be to ensure lawful processing. Processing will be done lawfully if all the (other) data protection principles are complied with.[57]

2.2.2 Purpose specification

The second core principle of data protection laws is that personal data may only be collected for specified and lawful/legitimate purposes[58] and may not subsequently be processed in ways that are

53 WBP a 7, 8 and 9.

54 Bygrave *Data protection laws* 58. According to the WBP *Memorie van toelichting* 77, outside the Netherlands, the term "fair" has served as a source for the development of "*behoorlijksregels op het terrein van de gegevensbescherming*".

55 See Bygrave *Data protection laws* 58.

56 On wrongfulness as an element of the law of delict in SA law, see ch 7 par 2.3.2.

57 As such, it is probably not necessary to spell out lawful processing as a specific data protection principle in an Act.

58 Some laws, such as the WBP and DP Act, stipulate that the purposes for which data are processed must be "lawful", whereas other legal instruments, such as the Directive and the Convention, stipulate that such (continued...)

incompatible with those purposes.

For example, the USA Privacy Act provides that when government agencies (data controllers) collect information from individuals (data subjects), they should be informed *inter alia* of the purpose for which the information is intended to be used and the routine uses the information could be put to.[59]

The USA Fair Credit Reporting Act follows the purpose specification principle by providing that consumer reporting agencies (data controllers) may only furnish consumer reports for the purposes authorised by the Act.[60] This Act also requires reporting agencies to maintain reasonable procedures to ensure that consumer reports are furnished only for permissible purposes, which include that the prospective user of the information must give a certified undertaking that the information in the report will not be used for any other purpose than the one for which the report was initially supplied.[61]

The OECD Guidelines have an explicit purpose specification principle which requires that the purpose for which personal data are being collected should be specified not later than at the time of data collection.[62] The Convention provides that personal data undergoing automatic processing should be stored for specified and legitimate purposes and not used in a way that is incompatible with those purposes.[63]

The Directive implements the principle of purpose specification by providing that personal data must be collected for specified, explicit and legitimate purposes and must not undergo further processing in

58(...continued)
purposes must be "legitimate" (see also Bygrave *Data protection laws* 61). The two terms are synonymous, but the term lawful is preferred in this thesis.

59 See ch 2 par 4.2.2.7.

60 See ch 2 par 4.3.2.3.

61 See ch 2 par 4.3.2.6.a.

62 A shortcoming in the OECD Guidelines is that they do not require that the purpose should be a legitimate one. See further ch 3 par 2.2.5.3.

63 Convention 108/1981 a 5. See ch 3 par 3.2.4.1.

a way that is incompatible with those purposes.[64] The purpose for which data are collected must be determined at the time of collection, and must be made known to the data subject at that time. Further processing of data that is incompatible with this purpose is not permitted.

The second principle of the DP Act also provides that personal data may be obtained only for one or more specified and lawful purposes, and may not be further processed in any manner that is incompatible with such purpose or purposes.[65]

The WBP implements the purpose specification principle by providing that the collection of personal data must be for specific, explicitly defined and legitimate purposes which must be established before any data are collected, and may not be vague, uncertain or illegitimate.[66] The purposes for which the data are collected are important with regard to every other aspect of the processing of the data, such as the nature of the data that may be collected, the length of time the data may be kept, and further processing that may be done.[67]

It is submitted that the purpose specification principle should be seen as a cluster of three principles:[68]

❒ The purpose(s) for which data are collected must be specified or defined.

It is submitted that the purpose for which personal data are being collected should be specified not later than at the time of data collection. The subsequent use of such data should be limited to the fulfilment of that purpose, or another that is compatible with it, and should be specified whenever there is a change of purpose. Although allowance could be made for changes in the

64 See ch 3 par 4.2.4.1. Also see ch 4 par 4.3.4.3 and ch 5 par 4.3.4.1.a.

65 See ch 4 par 4.3.4.3.

66 WBP a 7.

67 This is called *doelbinding*, ie, binding by purpose or objective (see further ch 5 par 4.3.4.1).

68 See Bygrave *Data protection laws* 61.

purpose, such changes should not be introduced arbitrarily. Application of this principle also implies that when data no longer serve the purpose for which they were originally collected, they should be erased or expressed in an anonymous form.

❒ The purposes for which data are collected must be lawful.

It is submitted that it should be a requirement that the purposes for which data are collected and further processed should be lawful. From the comparative research, it is evident that in general the following grounds are considered to be valid grounds for justifying data processing: The fact that the data subject has consented to the processing of data,[69] the fact that processing is necessary for compliance with a legal obligation to which the controller is subject,[70] the fact that processing is necessary in order to protect the vital interests of the data subject,[71] the fact that 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,[72] the fact that processing is necessary for the legitimate interests of the controller or third parties to whom the data are disclosed, except where such interests are overridden by the data subject's interests in his or her right to privacy and identity.[73] These grounds of justification for the processing of personal data can be summarised as (a) the consent of the data subject, (b) the maintenance and furtherance of a legitimate private interest and (c) the maintenance and furtherance of the public interest.[74]

❒ The purposes for which the data are further processed may not be incompatible with the

69 See, eg, OECD Guidelines par 7 (ch 3 par 2.2.5.1); Dir 95/46/EC a 7(a) (ch 3 par 4.2.4.2).

70 See, eg, Dir 95/46/EC a 7(c) (ch 3 par 4.2.4.2).

71 See, eg, Dir 95/46/EC a 7(d) (ch 3 par 4.2.4.2).

72 See, eg, Dir 95/46/EC a 7(e) (ch 3 par 4.2.4.2).

73 See, eg, Dir 95/46/EC a 7(f) (ch 3 par 4.2.4.2).

74 See ch 7 par 2.3.2.3 for a detailed discussion of these two grounds of justification.

purposes for which the data were first collected.[75]

It is submitted that the general rule should be that any subsequent use made of data should be compatible with the original stated purpose. In certain circumstances, for example with the consent of a data subject, or by the authority of law, an exception could be made to this rule.[76] Processing for historical, statistical and scientific purposes will generally not be considered to be incompatible,[77] provided that additional safeguards are in place to ensure, for example, that the data are only processed anonymously or by persons subject to a duty of confidentiality.[78]

As will be seen,[79] the application of this principle will result in the data processing being done lawfully, because of the presence of a ground of justification that justifies processing. It also ensures that the limits of this justification are closely defined.

2.2.3 Minimality

The third core principle of data protection laws is that the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data are gathered and further

75 Aspects of the purpose specification principle are also reflected in the principles traditionally referred to as the principle of limitation of collection and of use (see eg Bennett *Regulating privacy* 106–18; ch 3 par 2.2.5.1 and par 2.2.5.4).

76 See further ch 3 par 2.2.5.4 and par 4.2.4.1.

77 See Simitis 1981 *Am J Comp L* 583; 1995 *Iowa L R* 445. Also see ch 3 par 4.2.4.

78 An important purpose of these safeguards is to rule out the use of the data "in support of measures or decisions regarding any particular individual" (Dir 95/46/EC recitals par (29)).

79 Ch 7 par 2.3.2.3.

processed. In accord with Bygrave,[80] this principle is referred to as the principle of minimality.[81]

Not all the laws studied equally reflect this principle. The privacy laws in the USA, for example, do not deal extensively with this principle. The Privacy Act merely provides that government agencies should only maintain those records that are necessary to accomplish the stated purpose of the agency. [82]

However, the principle of minimality is clearly evident in the Directive's provision that personal data must not be excessive in relation to the purposes for which they are collected and/or further processed.[83] The Convention has a similar requirement, except that it relates only to the purposes for which data are stored.[84]

These provisions are directed at ensuring minimality at the stage of data collection, but both instruments also contain provisions directed at ensuring minimality subsequent to that stage.[85] These provisions require personal data to be erased or rendered anonymous once they are no longer required for the purposes for which they have been kept.[86] The Directive provides, for example, that personal data must not be stored in a form which permits identification of data subjects for longer than is necessary and member states must impose appropriate safeguards for personal data that are stored for longer periods

80 Bygrave *Data protection law* 59. Since this is a very important aspect of data processing, it is appropriate to distinguish 'minimality" from other aspects of the data quality principle (which will be discussed next) that relates to the relevance, accuracy and currency (up-to-datedness) of data. It should be recognised that the processing of unnecessary data can make processing wrongful (see further ch 7 par 2.3.2.3 and par 5).

81 It should be kept in mind that aspects of the minimality principle are reflected in the principles traditionally referred to as the principles of limitation of collection, limitation of use and data quality (see eg ch 3 par 2.2.5.1; 2.2.5.2; 2.2.5.4; 3.2.4.1 and Bennett *Regulating privacy* 106–109).

82 5 USC s 552a(e)(1).

83 Dir 95/46/EC a 6(1)(c) (see ch 3 par 4.2.4.1).

84 Convention 108/1981 a 5.

85 Bygrave *Data protection law* 60.

86 See ch 3 par 3.2.4.1 and par 4.2.4.1.

for historical, statistical or scientific use.[87]

The minimality principle is also manifest in one of the EU Directive's basic regulatory premises, namely that the processing of personal data is prohibited unless it is necessary for the achievement of certain specified goals.[88]

The third data protection principle of the UK DP Act implements the minimality principle by requiring that personal data must, *inter alia*, not be excessive in relation to the purpose or purposes for which they are being processed and that data must not be kept longer than necessary for the purposes for which they were collected.[89]

The WBP in similar vein provides that in principle personal data may only be processed if they are sufficient (*toereikend*)[90] and not excessive in relation to the purposes for which they were collected or subsequently processed.[91]

The minimality principle aims to ensure that the personal data held for a particular purpose are sufficient (or adequate),[92] but not more than sufficient for that purpose.[93] The requirement that the data must be "necessary" for the stated purpose reflects the idea that the data should not exceed what is necessary to fulfil the purpose of the processing. It should be recognised that the processing of unnecessary data

87 See ch 3 par 4.2.4.1.

88 Bygrave *Data protection law* 60 (see Dir 95/46/EC a 7 and 8 – see ch 3 par 4.2.4.2).

89 See ch 4 par 4.3.4.4.and par 4.3.4.6.

90 *Toereikend* can also be translated with adequate.

91 WBP a 11(1) (see ch 5 par 4.3.4.1.e).

92 This notion is similar to the notion found in the quality principle, namely that information that creates a false impression because all the relevant data are not included is inaccurate. However, as has been pointed out, it is not always possible to draw exact lines between the principles and one will find that some of them overlap (see fn 40).

93 Data will be "sufficient" or "adequate" if they satisfy or meet the requirements of the stated purpose.

renders data processing wrongful.[94]

Data controllers should seek to identify the minimum amount of information about each individual which is required in order to properly fulfil their purpose. If it is necessary to hold additional information about certain individuals, such information should only be collected and recorded in those cases.[95]

It is thus submitted that in accordance with the principle of minimality it should be required that personal data should be sufficient, but not excessive, in relation to the purposes for which they are collected and/or further processed, and that personal data should be erased or rendered anonymous once they are no longer required for the purpose for which they have been kept.[96]

This principle reflects, as does the next, that even where processing is taking place for a lawful purpose, the processing should be done within certain limits in order to be reasonable and thus lawful.

2.2.4 Quality

The fourth core principle of data protection laws is that personal data should be valid with respect to what they are intended to describe, meaning that the data should be relevant,[97] accurate and up to date

94 See further ch 7 par 2.3.2.3 and par 5.

95 See DPR *Guidelines* 61 (ch 4 par 4.3.4.4).

96 The argument can be made that the requirement that data should be relevant should be considered part of the "minimality" principle, because personal data that are excessive for the stated purpose should be considered irrelevant. In similar vein, the requirement of data protection laws that obsolete or "out of date" data should not be kept should then also be seen as part of the minimality principle, the argument being that if data are not up to date, they are no longer relevant. However, for present purposes these concepts are seen as part of the quality principle, which will be discussed below. The reason for this is that the inclusion of data that are irrelevant or not up to date also affects the quality of the data involved in the processing of personal data. Furthermore, in most of the laws studied these concepts are grouped with concepts like accuracy which form part of the quality principle.

97 On the issue as to whether "relevance" should be considered as part of the "minimality" principle, see fn 96.

with respect to the purposes for which they will be processed.[98]

The Privacy Act provides that government agencies must maintain all records about an individual with such accuracy, relevance, currency (timeliness / up to datedness) and completeness as is reasonably necessary to assure fairness to the individual. Prior to disseminating records, the agencies should make reasonable efforts to ensure that such records are accurate, complete, up to date, and relevant for agency purposes.[99]

The Fair Credit Reporting Act aims to ensure the quality of information in credit reports by imposing a duty on the furnishers of information to provide accurate information (which includes the duty to correct and update information and to provide a notice of disputed information).[100] Another important provision is that a credit report must indicate the fact that the consumer is disputing information in a report.[101] Also relevant is the requirement that a consumer reporting agency is obliged to follow reasonable procedures when preparing a report in order to ensure maximum possible accuracy of the information in the report.[102] The Act also prescribes that a credit report may not contain obsolete information.[103]

The data quality principle of the OECD Guidelines expressly requires that 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.[104] The principles of the Convention regarding the quality of data provide *inter alia* that personal data undergoing automatic processing should be

98 Bygrave *Data protection law* 62.

99 See ch 2 par 4.2.2.7.

100 See ch 2 par 4.3.2.10.

101 See ch 2 par 4.3.2.4.

102 See ch 2 par 4.3.2.6 .b.

103 See ch 2 par 4.3.2.4.

104 OECD Guidelines par 8 (see ch 3 par 2.2.5.2).

accurate and, where necessary, kept up to date.[105]

The Directive gives effect to the quality principle by providing that personal data must be accurate, complete and kept up to date. Furthermore, every reasonable step must be taken to rectify or erase inaccurate or incomplete and outdated data.[106]

The UK DP Act's third and fourth principles embody aspects of the quality principle of data protection by requiring that personal data must be relevant, accurate and, where necessary, kept up to date.[107] The relevance of data to a data user's purpose will be judged objectively in respect of each individual data subject.[108] As far as the accuracy of the data is concerned, the data protection principles are not contravened because of any inaccuracy in personal data if the data have been accurately recorded from information obtained by the data controller from the data subject or a third party and the data controller has taken reasonable steps to ensure the accuracy of the data. The purpose for which the data were obtained and further processed is taken into account in this determination. If the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data must also indicate that fact.[109] Under the DP Act, the obligation of data controllers to ensure accuracy is not an absolute one, but the issue is whether the data user has taken all reasonable steps to ensure accuracy. Whether or not a data controller would be expected to take such steps will be a matter of fact in each individual case.[110] The DP Act also requires that the data should be kept up to date "where necessary". The necessity for updating is determined by the purpose for which the data are held.[111]

105 Convention 108/1981 a 5 (see ch 3 par 3.2.4.1).

106 Dir 95/46/EC a 6(1)(c) (see ch 3 par 4.2.4.2).

107 See ch 4 par 4.3.4.4 and par 4.3.4.5.

108 See ch 4 par 4.3.4.4.

109 DP Act of 1998 sch 1 part II par 7 (see ch 4 par 4.3.4.5).

110 See ch 4 par 4.3.4.5.

111 See ch 4 par 4.3.4.5.

The WBP provides that in principle the personal data may only be processed if they are relevant (*ter zake dienend*),[112] correct and precise (*juist en nauwkeurig*). The relevance, correctness and preciseness of the data are again determined with reference to the purposes for which they were collected or subsequently processed. The WBP requires that the data controller must take the necessary (*nodige*) steps to ensure that the personal data are correct and precise.[113] In other words, this is not an absolute duty. The responsible party does not have to guarantee the correctness of the data. The sense of the term *nodige* is that the responsible party must take the steps reasonably necessary, taking into account the nature of the data, the level of the technology available, and the cost of the measures.[114]

It is submitted that in order to comply with the quality principle, data controllers must ensure that the personal data are

- relevant

  The requirement that the all the data included should be relevant[115] to the purpose for which they are to be used means that the data should be related to that purpose. For example, data concerning opinions or evaluative data may easily be misleading if they are used for purposes to which they bear no relation.[116]

112 WBP a 11(1) (see ch 5 par 4.3.4.1).

113 WBP a 11(2).

114 See ch 5 par 4.3.4.1.

115 Bing 1984 *Michigan Yb Int Legal S* 271, 276 argues 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. His argument reflects the minimality principle, ie that sufficient information should be included to make the processing valid. This again illustrates that it is not possible to completely separate the data protection principles (see also fn 40).

116 OECD Guidelines Explanatory Memorandum 30.

❒ accurate[117]

Data should be considered to be inaccurate if they are incorrect or misleading as to any matter of fact.[118] A mere opinion, which does not purport to be a statement of fact, should not be subject to challenge on the grounds of inaccuracy.[119] On the other hand, the fact that data are literally true should not be sufficient. The question should be whether the impression created by the data is correct. For example, where a credit reference agency states that a specific person has not paid his or her debts for three months, but neglects to mention that the person was unconscious during that period as a result of a car accident, the statement is factually true, but portrays a false image of the person as posing a bad credit risk.[120] Another example would be if the data controller records the fact that the data subject refused to pay for a product or service, but does not record that payment was refused because of dissatisfaction with the service or product.[121] In other words, the image created by the information should not be misleading and should give a complete picture of the person's situation.[122]

The quality principle should oblige data controllers to accept information only from reliable sources and to take such steps as are practicable to verify the information prior to subjecting it to processing.[123] It is submitted that the obligation of data controllers to ensure accuracy should not be an absolute one; data controllers should not be required to guarantee the

117 Also see ch 7 par 2.3.2.3 where it is explained that the processing of incorrect data infringes a person's identity.

118 DPR *Data Protection Act 1998* 14 (see ch 4 par 4.3.4.5).

119 Jay & Hamilton *Data protection* 63.

120 Coetser *Identiteit* 195–196; Neethling *Persoonlikheidsreg* 308.

121 This provision will not be complied with if the processor does not have sufficient data to form the correct image of the data subject (see WBP *Memorie van toelichting* 96).

122 Note that a distinction can also be made between "formal" and "material" accuracy. Formal accuracy relates to whether the information has been recorded correctly; material accuracy relates to whether the correct information has been recorded (Schreuders 1998 (2) *Priv & Inf* 52, 56).

123 Lloyd *Data Protection Act 1998* 60.

correctness of the data. The question should be whether the data controller has taken all reasonable steps to ensure accuracy, taking into account the nature of the data, the level of the technology available, and the cost of the measures.[124] Whether or not a data controller is expected to take such steps, should be a matter of fact in each individual case. Matters that should be considered are the significance of the inaccuracy and whether it has caused or is likely to cause damage or distress to the data subject. It should also be considered whether it was reasonable for the data controller to rely on the source of the information and what steps were taken to verify the information. Also relevant to consider is whether the data controller should reasonably have checked the information with the data subject. It should also be ascertained what procedures were taken to avoid and detect inaccuracies while entering data and for correcting inaccurate information that has been supplied.[125]

❒ up to date

It is submitted that data controllers should be obliged to keep data or information up to date only if it is "necessary".The necessity for updating should be determined by the purpose for which the data are held – for example updating is unnecessary if the data are part of a historical record, but is necessary if they are used for a purpose such as credit rating. Other factors which may play a role include whether a record is kept of the date when the information was recorded or last updated; whether all those involved with the data, including people to whom they are disclosed as well as employees of the data user, are aware that they do not necessarily represent the current position; whether the data user takes any steps to update the personal data, for example, by checking back at intervals with the original source or with the data subject; and whether the fact that the personal data are out of date is likely to cause damage or distress to the data subjects.[126] When data are no longer relevant or up to date, they should

124 See ch 5 par 4.3.4.1.

125 See ch 4 par 4.3.4.5.

126 See ch 4 par 4.3.4.5.

be considered to be "obsolete" and the data controller should be obliged to erase such data. The processing of irrelevant or outdated data cannot serve the purpose for which the data were collected and it is therefore unreasonable and thus wrongful to process such data.[127]

The requirements of relevance, accuracy and currency (up-to-datedness[128]) are all-important aspects of the quality principle. All these requirements should be linked to the purpose to be served by the data.[129] The issue should be whether or not harm can be caused to data subjects because of lack of accuracy and updating. These requirements should not be more far-reaching than is necessary for the purposes for which the data are used.[130] Compliance with the quality principle will ensure that the data processing does not exceed the limits of the applicable ground of justification.

2.2.5 Disclosure limitation

The fifth core principle of data protection laws is that data controllers' disclosure of personal data to third parties must be restricted, and that disclosure may occur only with the consent of the data subject or by authority of law.[131]

This principle is not always expressed in data protection instruments in the manner formulated above. Neither the Convention nor the EC Directive (and thus also neither the UK DP Act nor the Dutch WBP) specifically address the issue of disclosure limitation – these instruments treat it as part of the broader issue of the conditions for processing data. They treat it as part of the principles of fair and lawful processing and of purpose specification.

127 See Neethling *Persoonlikheidsreg* 331. See ch 7 par 2.3.2.3.

128 "Up-to-date" is also referred to as "timely" in some national legislation eg the UK Data Protection Act of 1984.

129 See OECD Guidelines Explanatory Memorandum 30.

130 Eg, historical data may often have to be collected or retained for long periods for social research (involving longitudinal studies of developments in society), historical research, or for archival purposes (see OECD Guidelines Explanatory Memorandum 30).

131 Bygrave *Data protection laws* 67.

However, there is merit in Bygrave's view[132] that it is justifiable to single out disclosure limitation as a principle in its own right. Bygrave indicates that the principle of disclosure limitation plays a distinct and significant role in shaping data protection laws, and numerous national statutes expressly delineate it as a separate principle or set of rules.[133]

The US Privacy Act contains specific provisions relating to the conditions under which government agencies may disclose personal information, as well as provisions relating to an account that must be kept of such disclosures.[134] In fact, the most important provision of the Privacy Act, is section 552a(b), which provides that no federal agency may disclose any record contained in a system of records by any means of communication to any person or to another agency unless (a) the individual to whom the record pertains has, before such disclosure, requested or consented to such disclosure in writing; or (b) such disclosure falls within one of the listed exceptions.[135] Violation of this section may lead to civil liability or criminal penalties.[136]

The OECD Guidelines (in a principle referred to as "use limitation") provides that personal data should not be disclosed or made available for purposes other than those specified in accordance with the purpose specification principle, except (a) with the consent of the data subject or (b) by the authority of law.[137]

It is submitted that effect should be given to the disclosure limitation principle by providing that data controllers' disclosure of personal data to third parties should be restricted to disclosure that accords

132 Bygrave *Data protection laws* 67. Bygrave (fn 257) states that the data protection laws of Canada, New Zealand and Australia contain this principle.

133 See eg Canada's federal Privacy Act (1982), the New Zealand Privacy Act (1993) and the Australian Privacy Act (1988).

134 See ch 2 par 4.2.2.4. and 4.2.2.5.

135 5 USC s 225a(b)(1)–(12). See further ch 2 par 4.2.2.4.

136 See ch 2 par 4.2.2.13 and par 4.2.2.13.

137 OECD Guidelines par 10 (see ch 3 par 2.2.5.4).

with the purpose specification principle, unless the data subject has consented or the disclosure is authorised by law.[138] To supplement this principle it should also be required that an account should be kept of any disclosures made.

2.2.6 Data subject participation

The sixth core principle of data protection laws is that subjects should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or organisations.[139]

The Privacy Act complies with the data subject principle by providing that a government agency (data controller) should, upon request by a data subject (an individual), permit such individual access to any information on him or her, and permit the individual to request amendment of a record that is incorrect or misleading. If the government agency refuses to amend the record the individual must be informed of the reason for such refusal and the procedures for review of the refusal. If the agency still refuses to amend the record after review, the individual can file a statement setting out that he or she disagrees with the controller about the accuracy of the record, in which case the data controller must, in all subsequent disclosures, clearly note the disputed part of the record and provide a copy of the statement of disagreement.[140]

The Fair Credit Reporting Act also contains extensive provisions aimed at allowing the consumer (data

138 Bygrave *Data protection laws* 67.

139 Bygrave *Data protection laws* 63. Bygrave's formulation of the principle of "data subject participation and control" embraces aspects of what the OECD Guidelines call the "individual participation principle" as well as aspects that are traditionally included in a principle referred to as the principle of "openness or transparancy" (see eg Bennett *Regulating privacy* 101; Roos *Data protection* 43). Because of the importance of the notion that data processing should be open, it is preferred in this thesis to discuss the openness principle as a core data protection principle separate from the data subject participation principle.

140 See ch 2 par 4.2.2.6.

subject) access to his or her files[141] and to dispute information in such files, as well as provisions that third parties who have received disputed information must be informed about the dispute.[142]

According to the OECD Guidelines' individual participation principle, data subjects should have the right to obtain from a data controller, or in another manner, confirmation of whether or not the data controller has data relating to them, and to have such data communicated to them within a reasonable time, in a reasonable manner and at a fee that is not excessive. The form should also be readily intelligible to the data subjects. Furthermore, data subjects should have the right to be given reasons if a request is denied and to be able to challenge such denial. Data subjects 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. This principle thus entails a right to access, a right to reasons and a right to challenge.[143]

The Convention requires that any person should 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 file are;[144] 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;[145] be able to obtain either rectification or erasure of personal data that have been processed contrary to the provisions of domestic law giving effect to the basic principles of the Convention;[146] and have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure is not

141 See ch 2 par 4.3.2.7.

142 See ch 2 par 4.3.2.8 for a complete discussion of these provisions.

143 See ch 3 par 2.2.5.7.

144 Convention 108/1981 par 8(a).

145 Convention 108/1981 a 8(b).

146 Convention 108/1981 a 8(c).

complied with.[147]

The Directive confers on the individual a right to participate in the processing of data by requiring that every data subject must have the right of access to data relating to such data subject, personally and 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; 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.

The right to access data under the Directive actually entails three separate rights. First, the right of data subjects to obtain confirmation on whether or not data relating to them are being processed as well as information at least on the purpose(s) of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data will be disclosed. Second, the right to obtain, in an intelligible form, the data undergoing processing and any available information as to their source. Third, 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).[148]

Also relevant in this regard is the right of data subjects to object to the processing of data relating to them to which they have not consented (that is, processing carried out in the public interest or for the promotion of the legitimate interests of the controller or third parties to whom the data will be disclosed).

The right to object also exists where data are processed for direct marketing purposes.[149] The Directive provides that data subjects must have a right to object to the processing of data for direct marketing

147 Convention 108/1981 a 8(d). See further ch 3 par 3.2.4.4.

148 See ch 3 par 4.2.4.6. See ch 4 par 4.3.5.1, par 4.3.5.6 and ch 5 par 4.3.8.1, par 4.3.8.2.

149 See ch 3 par 4.2.4.7. See ch 4 par 4.3.5.2, par 4.3.5.3 and ch 5 par 4.3.8.3.

purposes, at no cost and without having to give reasons. 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 such purposes.[150] The Directive does not prescribe the mechanism by which this should be implemented – that is, whether an "opt in" or "opt out" system should be used.[151] 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.[152]

Another relevant provisions is the one granting the data subject the right not to be subjected to automated decisions (profiling).[153] As indicated,[154] profiling means the inference of a set of characteristics about the behaviour of an individual person or collective entity and the subsequent treatment of that person or entity or other persons or entities in the light of these characteristics.

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, and which is based solely on automated processing of data intended to evaluate certain related personal aspects, such as performance at work, creditworthiness, reliability, and conduct.[155]
This article is designed to protect the individual against the perceived growth of automatisation of organisational decisions about individuals.[156] Note, however, that this provision restricts a particular

150 See ch 3 par 4.2.5.7.

151 Bennett *Data protection directive* 5.

152 See in this regard, the discussion of "spam" in ch 1 par 1.3.

153 See ch 3 par 4.2.4.8. Also see ch 4 par 4.3.5.4 and ch 5 par 4.3.8.4. Also see Bygrave *Data protection law* 301–362 for an extensive discussion of the issue of profiling in the context of data protection.

154 Ch 1 par 1.3.

155 Dir 95/46/EC a 15.

156 See ch 3 par 4.2.4.8.

application of profiling, but does not prohibit profiling.[157]

The sixth principle of the DP Act requires that personal data must be processed in accordance with the rights of data subjects under the DP Act. These rights include the right of a data subject to have access to his or her personal data; a right to prevent processing that is likely to cause damage or distress; a right to prevent processing for purposes of direct marketing and a right to object to automated decision-taking.[158]

The DP Act implements the right to object to direct marketing by means of an "opt out" system.[159] However, a further requirement of the Directive, namely that data subjects must be informed of the transfer of data, for direct marketing purposes, to third parties, is not present in the DP Act of 1998, which is a significant limitation of the rights being granted to the data subject.[160] The DP Act implements the provision relating to profiling or automated decision making by requiring the data subject to notify a data controller in writing that the controller must ensure that no decision which significantly affects him or her is based solely on the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to such individual.[161]

The WBP gives effect to the principle of data subject participation by providing that data subjects have a right to have access to their personal data (which includes the right to obtain confirmation as to whether or not data relating to them are being processed, the right to obtain access to the personal data undergoing processing, and the right to obtain information concerning the underlying logic of the automated processing of the data); the right to request correction of such data; as well as with the right to object to the processing of their data where they have not consented, or where processing takes

157 For an extensive discussion of a Dir 95/46/EC a 15, see Bygrave *Data protection law* 319–328.

158 See ch 4 par 4.3.4.7.

159 See ch 4 par 4.3.5.3.

160 Chalton et al *Encyclopedia of data protection* par 1–246/2.

161 See ch 4 par 4.3.5.4.

place for direct marketing purposes. In the case of processing for direct marketing, the WBP uses an "opt-out" system . The Dutch legislator decided to put the burden on the data subjects to object, because an "opt-in" system would have been too burdensome for the data controllers from a financial point of view.[162] The WBP also contains a provision that data subjects may not be subjected to automated decision making.[163] The WBP provides that persons may not be subjected to decisions involving legal consequences for them, or which affect them to a substantial degree, where these decisions have been taken solely on the basis of the automated processing of personal data intended to provide a picture of certain aspects of their personality. It allows for two exceptions.[164]

In the light of the above, it is submitted that the principle of subject participation entails the following aspects:

- Data subjects must have a right to have access to their personal data at reasonable intervals and without excessive delay or expense.

  This right entails three aspects, namely
  - the right to obtain confirmation as to whether or not data relating to them are being processed as well as information at least on the purpose(s) of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data will be 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 information concerning the underlying logic of the automated

162 However, if the data controller intends to give the information to third parties or use it on behalf of third parties for direct marketing purposes, the data subjects must be notified of this and of the possibility of objecting. In such a case the notification must be made via a suitable newspaper, or in some other appropriate form. Where the data are regularly used for direct marketing purposes, this notification should be done once a year (see ch 5 par 4.3.8.3).

163 See ch 5 par 4.3.8.

164 See ch 5 par 4.3.8.4.

processing of the data, at least in the case of automated decisions

❒ Data subjects must have the right to request correction, erasure or blocking[165] of incomplete or inaccurate personal data, or data the processing of which otherwise does not comply with the data protection principles or which otherwise infringes a legal provision.[166] 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.[167] If requested to do so, the data controller must also notify the data subjects of the third parties to whom the information has been disclosed.[168]

❒ Data subjects must have the right to object to the processing of their data where they have not consented to such processing.

❒ Data subjects must have the right to object to processing of personal data for direct marketing

165 "Rectify" means to put a record straight. "Blocking" in the context of data processing means that the controller makes the data inaccessible, although the data remain on record. "Erasure" and "destruction" have the same effect, but they envisage different activities. Data are destroyed if the medium on which the data are held is physically destroyed. However, where the medium contains other data which are not inaccurate and should not be destroyed, the offending data should be removed by erasure, leaving the remainder of the record intact (see Jay & Hamilton *Data protection* 230–232; also see Bainbridge *Data protection law* 138).

166 Where personal data have been recorded on a data medium to which no modifications can be made, such as CD-ROM or microfiche, the responsible parties must take the necessary steps to inform the data user that it is impossible to correct, supplement, delete or screen the data, even where there are grounds for modifying the data. In such a case it may be required that the permanent medium be updated by means of another, less permanent source, in which corrections that should be made to the permanent source are noted. Persons using the permanent source must then be referred to the additional source to ensure that they have the correct information (see further ch 5 par 4.3.8.2).

167 A balancing of interests must take place in which the nature of the correction plays an important role in determining the extent of the duty to inform third parties about corrections. Eg, corrections to criminal data, indicating that a person was found not guilty, would require that even third parties who received the information a long time ago should be traced. However, a mere correction in an address would not impose the same burden (see further ch 5 par 4.3.8.2).

168 WBP a 38(2).

purposes.[169]

- ❒ Data subjects must have the right to object to the processing that will result in their being subjected to automated decision making.[170]

- ❒ Data subjects must have a remedy to enforce their rights to participate.

The data subject participation principle is necessary for the effective and equitable control of data processing.[171] The "classic trio" of data subject rights, namely "the right to know, the right to correction and erasure and the right to a remedy in the case of refusal" has been described as "the most important legal innovation which data protection has achieved, both in domestic law and in international law".[172]

2.2.7 Openness or transparency

The seventh principle, as formulated by the OECD Guidelines, requires that there should be a general policy of openness about developments, practices and policies in respect of personal data. As Bennett puts it: "The very existence of record-keeping systems, registers or data banks should be publicly known."[173] Data subjects should be made aware of the fact that their personal data are being processed, the purpose(s) for which this is done, the identity of recipients of their personal data, as well as the identity and usual residence of the data controller.[174] According to the OECD Guidelines, the openness principle can be complied with in any one of several ways, examples of which are: (a) regular

169 In an ideal world, the "opt-in" system would be preferable. However, in order to strike an appropriate balance between the right of privacy of persons on the one hand and the right of other parties to pursue legitimate business interests, the "opt-out" system should be implemented.

170 See ch 3 par 4.2.4.8 for a discussion of this aspect.

171 This principle is reflected in active control measures of data protection as formulated by Neethling *Persoonlikheidsreg* 334 (see ch 7 par 3.2).

172 Hondius 1983 *Neth Int L R* 103, 116–117.

173 Bennett *Regulating privacy* 101–103.

174 See ch 3 par 2.2.5.6.

information from data controllers to data subjects; (b) publication in official registers of descriptions of activities concerned with the processing of personal data; and (c) registration by data controllers with public bodies.[175] The Convention does not contain a specific provision that relates to this principle.

The Privacy Act complies with this principle in two ways: (a) by requiring data controllers to publish a notice at least once a year in the Federal Register disclosing the existence and nature of each system of records,[176] and (b) by requiring the data controller to supply a statement, at the time when the information is collected, of the authority on which the information is solicited, the principal purposes for which it will be used, routine uses, and the effect on the data subject if he or she does not provide the information.[177] The requirement that every data controller should promulgate rules to facilitate access by data subjects to all systems of records also helps to publish the existence of data banks.[178] Also relevant is the provision that when information could result in an adverse decision about individual rights or benefits, such information should be collected directly from the individual as far as is possible.[179]

The Fair Credit Reporting Act does not in general require consumer reporting agencies (data controllers) to inform consumers (data subjects) that they have files on them or that a consumer report on them has been requested.[180] In many instances, however, the consumer will know of the existence of a credit file on him or her owing to other provisions of the Fair Credit Reporting Act. First of all, a consumer must be informed about the fact that a consumer report on him or her has been requested where such a report is requested for employment purposes, or in connection with a credit or insurance transaction not initiated by the consumer (in these cases the consumer's authorisation must first be

175 OECD Guidelines Explanatory Memorandum 31.

176 5 USC s 552a(e)(4).

177 5 USC s 552a(e)(3) (see ch 2 par 4.2.2.7).

178 5 USC s 552a(f) (see ch 2 par 4.2.2.8).

179 5 USC s 552a(e)(2) (see ch 2 par 4.2.2.7).

180 See ch 2 par 4.3.2.7.

obtained).[181] Furthermore, a duty rests with the person procuring an investigative consumer report to inform the consumer that such a report may be made.[182] Where a person takes an adverse action with respect to a consumer based on information contained in a consumer report, such person must also notify the consumer of such action, and must inform the consumer of the name, address and telephone number of the consumer reporting agency that furnished the report to the person.[183] Further, a person who uses a consumer report to solicit a credit or insurance transaction must, with each written solicitation to the consumer, clearly state that information contained in the consumer's consumer report was used in connection with the transaction.[184]

The Directive implements the openness principle by requiring (a) that data controllers must furnish certain information to their countries' supervisory authorities and that this information should be published in a register of processing operations; and (b) that certain information should be given to the data subject. The purpose of the notification procedure, coupled with the publication of the information in a register, is to promote transparency regarding the processing of personal data. The right of the data controller to process data for a legitimate purpose and the right to privacy of the data subject have to be balanced against each other, and the notification process ensures that this balancing is subject to supervision.[185]

First, a data controller or its representative must notify the supervisory authority before carrying out any automatic (or partly automatic) processing operation intended to serve a single purpose or several related purposes.[186] The controller must supply its name and address and that of its representative, the purpose or purposes of the processing, a description of the category or categories of data subjects and

181 15 USC s 1681b(c)(1)(A) (see ch 2 par 4.3.2.3.c).

182 See ch 2 par 4.3.2.5.

183 15 USC s 1681m(a)(2)(A) (see ch 2 par 4.3.2.9.a).

184 15 USC s 1681m(d)(2) (see ch 2 par 4.3.2.9.c).

185 See ch 5 par 4.3.6.

186 Dir 95/46/EC a 28.

of the data or categories of data relating to them, the recipients 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.[187] The notification process may be simplified or exempted by individual member states in a few cases only.[188]

Second, the supervisory authority must keep a register of processing operations about which it has been notified. The information contained in the notification sent to the supervisory authority must be included in the register. The register must be open for inspection to any person. 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.[189]

Third, data controllers have a duty to keep data subjects informed. Data controllers must inform data subjects about the identity of the controllers and their representatives, and the purposes of the processing for which the data are intended. Further information, such as the categories of data concerned, the recipients of the data, whether replies to the questions are obligatory or voluntary, the possible consequences of failure to reply, and the existence of the right of access to data and the right to rectify such data if they are incorrect, 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.[190]

In the UK, the DP Act provides that no processing of personal data may take place unless an entry in respect of the data controller is included in a register maintained by the Commissioner (data protection

187 Dir 95/46/EC a 19.

188 Dir 95/46/EC a 18(2) (see ch 3 par 4.2.4.10.a). Also see ch 4 par 4.3.7 and ch 5 par 4.3.6.

189 Dir 95/46/EC a 21(3) (see further ch 3 par 4.2.4.10.c).

190 Dir 95/46/EC arts 10 and 11(1) (see ch 3 par 4.2.4.5).

authority).[191] It is an offence to process personal data without notification, unless the processing is exempt from notification.[192] Any data controller who wishes to be included in the register maintained by the Commissioner is obliged to give a notification to the Commissioner.[193] The notification must specify what the Act calls "the registrable particulars" (such as the name and address of the data controller and its representative, a description of the personal data being processed, a description of the category or categories of data subjects to which the data relate, a description of the purpose(s) for which the data are to be processed and a description of recipients to whom the data controller intends to disclose the data) as well as a general description of the security measures taken to protect the personal data.[194] Data controllers may be exempted from notification in certain circumstances, but remain under an obligation to provide the same information as is contained in the registrable particulars, upon receiving a written request for such particulars from any person.[195] The Commissioner is obliged to maintain a register of persons who have given notification.[196]

The DP Act also provides that in order to process data fairly, the data controller must ensure as far as is practicable that the data subject had certain information, or was provided with such information, or that such information was made readily available to the data subject.[197] The information that must be supplied is the identity of the data controller, the identity of any nominated representative, the purpose or purposes for which the data are intended to be processed, and any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed,

191 DP Act of 1998 s 17(1).

192 DP Act of 1998 s 21(1).

193 DP Act of 1998 s 18(1).

194 See ch 4 par 4.3.7.

195 DP Act of 1998 s 24(1) (see ch 4 par 4.3.7.5).

196 DP Act of 1998 s 19(1).

197 DP Act of 1998 sch 1 part II par 2(1)(a).

to enable processing in respect of the data subject to be fair.[198] Where the data were not obtained directly from the data subject the data controller must also ensure that the data subject has such information as soon as is practicable.[199]

The WBP provides that the data controller must notify the data protection authority before carrying out any automated (or partly automated)[200] processing operation intended to serve a single purpose or different related purposes.[201] Non-automated processing should also be reported if it is subject to a prior investigation, in other words, if it poses a risk to privacy.[202] The data protection authority must maintain an up-to-date register of the data processing reported to them. The register must be open to any person for inspection at no cost. Where the processing is not subject to notification, the data controller must make the relevant information available to any person who so requests, except in a case where the exemption from notification was for the gathering of criminal data and was given by general administrative order, or in the case of public registers set up by law.[203]

In the light of the above, it is submitted that the principle of openness entails the following:

- There must be an obligation on a data controller to notify the data protection authority of its intention to carry out any automated or partly automated processing operations intended to serve a single purpose or different related purposes, before such processing takes place.[204]

198 DP Act of 1998 sch 1 part II par 2(3).

199 DP Act of 1998 sch 1 part II par 2(1)(b) (see ch 4 par 4.3.4.2).

200 WBP a 27(1).

201 WBP a 27(3).

202 WBP a 27(2).

203 WBP a 30(4) (see ch 5 par 4.3.6.2).

204 As a general rule non-automated processing need only be notified if it is likely to create specific risks to the right of privacy of data subjects, eg where a personal identification number is processed for a different purpose than the one for which it is specifically intended, or where criminal data are processed (see further ch 5 par 4.3.6.1 read with par 4.3.6.3).

- ❒ The data protection authority must maintain an up-to-date register of the data processing reported to it, which register must be open to any person for inspection at no cost.

- ❒ There must be a duty on data controllers to keep data subjects informed about the identity of the controllers and their representatives, and the purposes of the processing for which the data are intended.

The openness principle ensures that individuals know about and can participate in enforcing their rights under a data protection regime.[205]

2.2.8 Sensitivity

The eighth core data protection principle is "sensitivity".[206] The principle of sensitivity holds that the processing of certain types of data which are regarded as especially sensitive for data subjects, should be subject to more stringent controls than other personal data. This principle is manifested primarily in rules that place special limits on the processing of predefined categories of data.[207]

Attempts to single out particular categories of data for special protection independent of the context in which the data are processed have been controversial.[208] The OECD Guidelines do not, for example, contain extra safeguards for designated categories of data. The absence of such safeguards for sensitive data is, according to Bygrave, due partly to failure by the Expert Group responsible for drafting the Guidelines to achieve consensus on which categories of data deserve special protection, and partly to a belief or common assumption that the sensitivity of personal data is not an *a priori* given but is

205 See the principle of subject participation (par 2.2.6).

206 Bygrave *Data protection laws* 68–69.

207 Bygrave *Data protection laws* 68.

208 Bygrave *Data protection laws* 69.

dependent on the context in which the data are used.[209]

The Convention contains a provision regarding sensitive personal data: Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, or relating to criminal convictions, may not be processed automatically unless the domestic law provides appropriate safeguards,[210] in other words safeguards that are suitable for or adapted to the specific type of sensitive data involved.[211] The list is not meant to be exhaustive, and a contracting state may include other categories in its domestic law.[212]

The list of sensitive data categories in the Directive,[213] on the other hand, is intended to be exhaustive. It includes data on a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health and sexual life. As a general rule, the Directive requires member states to prohibit the processing of personal data that are included in the list of data considered to be of a "sensitive" nature. Processing of sensitive data may be permitted as an exception to this general rule only if: (a) the data subject has explicitly consented thereto; or (b) if one of a specific list of grounds justifying such processing is present.[214] Member states may also "for reasons of substantial public interest" lay down additional exemptions, provided that "suitable safeguards" are introduced.[215] In such a case the member state must notify the Commission of such an exemption.[216]

209 Bygrave *Data protection laws* 69.

210 Convention 108/1981 a 6.

211 In the case of medical data, eg, it can be required the data should only be processed by a medical practitioner or a person subject to a duty of confidentiality.

212 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. See further ch 3 par 3.2.4.2.

213 Dir 95/46/EC a 8(1) (see ch 3 par 4.2.4.3).

214 See ch 3 par 4.2.4.3.

215 Dir 95/46/EC a 8(4). "Suitable" is synonymous with "appropriate".

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

The Directive also contains special provisions for data on criminal records. 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 a national law that provides suitable, specific safeguards.[217] In this instance the Commission must also be notified of the derogation.[218] However, a complete register of criminal convictions may only be kept by an official authority.[219] Member states may (but are not obliged to) provide that data relating to administrative sanctions or judgments in civil cases should also be processed under the control of official authority.[220]

The Directive does not prohibit the use of a national identification number, but leaves it to member states to determine the conditions under which such a number may be processed.[221] As regards freedom of expression, the Directive requires member states to make provision for exemptions or derogations from certain provisions (namely 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 such exemptions are necessary in order to reconcile the right to privacy with the rules governing freedom of expression.[222]

---

217 This exemption was included on the insistence of Britain which 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* par 139).

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

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

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

221 Dir 95/46/EC a 8(7). Not all countries have a national identification card system in place. Examples of countries that do have a national identification card are Belgium, Egypt, France, Germany, Greece, Hong Kong, Malaysia and the Republic of South Africa. Countries such as India, Ireland, the Netherlands, New Zealand, the UK, the USA and the Nordic countries do not have a national identification card. In the UK consultations started in 2002 on the possibility of introducing an "entitlement card". The USA has a social security number, but this is used by government only to administer social security benefits (see also EPIC *Privacy and human rights* 27).

222 Dir 95/46/EC a 9 (see further ch 3 par 4.2.4.4).

The UK DP Act and the Dutch WBP both give effect to these provisions of the Directive.[223] A provision of the WBP which deserves special mention is the exception made for the processing of sensitive personal data where the processing is for scientific research or statistical purposes. Such research should be in the general interest, the processing of the data should be necessary for the particular research or statistics, it should be impossible or should involve a disproportionate effort to ask for express consent, and sufficient guarantees should be provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.[224] The WBP furthermore provides that the prohibition on the processing of sensitive data is not applicable if processing is necessary for journalistic, artistic or literary purposes.[225] As regards the use of a national identification number, the WBP provides that when a law prescribes that a number will be associated with a person in order to identify that person, that number may be used only when processing personal data to give effect to the provisions of that Act or to achieve the aims of that specific Act.[226]

The UK DP Act provides for an exemption from the prohibition on processing of sensitive data in the case of processing for "special purposes". "Special purposes" refers to processing for the purposes of journalism as well as artistic and literary purposes. The processing activities are exempted from the data protection principles and the subject access provisions.[227]

The Privacy Act provides that government agencies may not maintain a record describing how any individual exercises rights guaranteed by the First Amendment (in other words, relating to freedom of speech), unless expressly authorised by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorised law enforcement activity.[228] Special

223 For a complete discussion of these provisions, see ch 4 par 4.3.4.2 and ch 5 par 4.3.4.2.

224 WBP a 23(2) (see ch 5 par 4.3.4.2).

225 WBP a 3(2).

226 WBP a 24(1).

227 See ch 4 par 4.3.6.2.

228 See ch 2 par 4.2.2.7.

provisions are also made with regard to mailing lists and the use of social security numbers.[229] An agency may not sell or rent an individual's name and address as part of a mailing list, unless specifically authorised by law.[230] Section 7 of the Privacy Act makes it unlawful for a federal, state or local agency to deny an individual any right, benefit or privilege provided by law because of the individual's refusal to disclose his or her social security number. An agency that requests a social security number must inform the individual whether disclosure is voluntary or mandatory, under what authority it is solicited and what uses will be made of it.[231]

The Fair Credit Reporting Act considers medical information to be worthy of extra protection, and prohibits the inclusion of such information in a consumer report obtained for employment purposes, or for a credit or insurance transaction, unless the data subject (consumer) has consented to the furnishing of the report.[232]

In the light of the above it can be said that the data protection principle of sensitivity requires that the processing of sensitive data (that is, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life) must as a general rule be prohibited, and should only be allowed in exceptional cases. Processing of sensitive data may, for example, take place[233]

- to allow data controllers to carry out legal obligations (for example, in the area of employment law)
- if it 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
- where it is done by a foundation, association or any other non-profit-seeking body for political,

229 See ch 2 par 4.2.2.11 and par 4.2.2.12.

230 5 USC s 552a(n).

231 Pub L No 93–579, s 7(b), 88 Stat 1897 (1974).

232 15 USC s 1681b(g) (see ch 2 par 4.3.2.3).

233 Dir 95/46/EC a 8(2).

philosophical, religious or trade-union purposes

- ❒ if the processing relates to data which are manifestly made public by the data subject
- ❒ if the processing is necessary for the establishment, exercise or defence of legal claims
- ❒ if the processing is done solely for journalistic, literary and artistic purposes and such processing is necessary to give effect to the rules governing freedom of expression

This principle also requires that special provisions should be in place for the processing of data pertaining to criminal convictions and for the processing of national identification numbers.[234]

2.2.9 Security and confidentiality

The ninth core data protection principle, the security principle, is formulated by the OECD Guidelines as follows: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.[235] 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. "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 unauthorised input of data. "Use" includes unauthorised copying.[236]

In this regard the Privacy Act requires that each data controller (agency) should establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records

234 The use of such a number should be closely regulated. Critics of a national identification card-system point out that such cards, especially when combined with information contained in databases, enable the profiling of individuals and create a misplaced reliance on a single document, which enables precisely the type of fraud the cards are meant to eliminate (EPIC *Privacy and human rights* 28).

235 OECD Guidelines par 11 (see ch 3 par 2.2.5.5).

236 OECD Guidelines Explanatory Memorandum 31 (see ch 3 par 2.2.5.5).

and to protect them against anticipated threats or hazards to their security or integrity.[237] The Fair Credit Reporting Act does not contain provisions of this nature.

The Convention's provisions regarding security measures provide that appropriate 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.[238] "Appropriate security measures" means that the measures should be adapted to the specific function of the file and the risks involved.[239] 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.[240]

The Directive aims to ensure both the confidentiality and security of data processing. As regards the confidentiality of data processing, it requires member states to prohibit the processing of data by a data processor, unless the data processor has been instructed to do so by the data controller or is required to do so by law. 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 against 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 against all other unlawful forms of processing. 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 the state of the art, the cost of implementation, and the nature of

237 See ch 2 par 4.2.2.7.

238 Convention 108/1981 a 7 (see ch 3 par 3.2.4.3).

239 Convention 108/1981 Explanatory Report par 57.

240 Convention 108/1981 Explanatory Report par 49.

the data to be processed.[241] Should the controller choose a processor to do the processing on its behalf, the controller remains responsible for security and is required to choose a processor that provides sufficient guarantees in respect of the technical and organisational security measures. The data controller must also complete a written contract with the processor, stipulating that the processor will act only on instructions from the controller, and that the security provisions are also applicable to the processor.[242]

The seventh principle of the UK DP Act requires that appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The obligations imposed by this principle are reinforced by an obligation to notify the Commissioner of the security measures in place.[243]

The WBP contains extensive provisions, in line with those of the EU Directive, regarding the implementation of the principle of confidentiality and security of processing. First, any processing of data by anyone acting under the authority of the data controller or the processor, as well as by the processors themselves, is prohibited unless ordered by the data controller or required by law.[244] If a duty of confidentiality under official, professional or legal provisions does not already apply to a data processor, processors must treat as confidential the personal data which come to their knowledge, except where they are required to communicate such data by provision of the law or in connection with

241 "Appropriate security measures" indicates in the first instance that the measures should be suited to the data processing activity taking place and the risks involved (see Convention 108/1981 Explanatory Report par 57). Secondly, it indicates that the security measures should reflect the state of the technology. The legislator cannot prescribe more precisely the measures to be taken, because they change with time and more precise instructions may therefore restrict the level of protection (see WBP *Memorie van toelichting* 99).

242 See ch 3 par 4.2.4.9.

243 DP Act of 1998 s 18(2)(b). However, this principle seems to fall short of the requirements of the Directive – the Directive's emphasis on the need for security in particular where the processing involves the transmission of data over a network has been left out eg, as well as the requirement that a processor may act only on instructions from the controller. Neither does the UK Act contain provisions relating to confidentiality. See further ch 4 par 4.3.4.8.

244 WBP a 12(1).

their duties.[245] Furthermore, the responsible party must implement appropriate technical and administrative measures to secure personal data against loss or against any form of unlawful processing. The measures should guarantee a level of security that is appropriate to the risks presented by the processing and the nature of the data to be processed. Factors that are relevant in determining the appropriateness of the measures are the state of the technology and the cost of implementation.[246] Should the responsible parties choose a processor to do the processing on their behalf, the responsible parties remain responsible for security and must choose a processor that provides adequate guarantees concerning the technical and administrative security measures applicable to the processing that will be carried out. The responsible party must ensure that the prescribed measures are complied with.[247] The processing activities of the processor must be governed by an agreement or another legal act whereby a contract is created between the responsible party and the processor.[248] In order to serve as evidence, the parts of the agreement or legal act relating to personal data protection and the security measures referred must be in writing or in an equivalent form.[249]

It is submitted that the provisions of the WBP address all the aspects of the principle of confidentiality and security and therefore provide a good example as to how this principle should be implemented. Security and confidentiality are very important aspects of data protection that should not be neglected.

2.2.10 Accountability principle

The tenth and last core principle of data protection is that a data controller should be accountable for compliance with measures which give effect to the principles stated above. According to the OECD

245 WBP a 12(2).

246 WBP a 13.

247 WBP a 14(1).

248 WBP a 14(2).

249 WBP a 14(5) (see further ch 5 par 4.3.4.1.f).

Guidelines Explanatory Memorandum,[250] 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 data processors are carrying out the data processing activities on their behalf.

The Privacy Act holds the agency accountable for compliance with the Privacy Act and affords remedies to the individual to enforce the Act.[251] The Privacy Act also imposes penal sanctions on officers or employees of agencies for wilful disclosure of agency records containing individually identifiable information, while knowing that such disclosure is prohibited by the Act, and for maintaining a system of records without meeting the notice requirements of the Act.[252]

The Fair Credit Reporting Act gives a consumer the right to bring a civil action against an agency or user who willfully, knowingly or negligently fails to comply with any requirement of the Act.[253] An officer or employee of the agency who knowingly and wilfully gives out information to a person not authorised to receive that information, and a person who obtains information under false pretences, can be fined or imprisoned.[254] The Fair Credit Reporting Act also gives powers to the Federal Trade Commission (FTC) and states to enforce the Act.[255]

The Directive provides that individuals must be entitled to a judicial remedy, in addition to any administrative remedy, for an infringement of the rights guaranteed by the national law applicable to the processing of personal data.[256] They must also be entitled to receive compensation from the controller

250 OECD Guidelines Explanatory Memorandum 32. See ch 3 par 2.2.5.8.

251 See ch 2 par 4.2.2.13.a.

252 See ch 2 par 4.2.2.13.b.

253 See ch 2 par 4.3.2.11.

254 See ch 2 par 4.3.2.12.

255 See ch 2 par 4.3.2.13.

256 See also the security and confidentiality principle discussed above, where it was pointed out that the data (continued...)

for damage suffered as a result of an unlawful processing operation or of any act incompatible with such laws. The national data protection legislation must also lay down the sanctions to be imposed in the event of any infringement of its provisions.[257]

The DP Act makes every data controller responsible for complying with the data protection principles in relation to all personal data in respect of which he or she is the data controller.[258] The Act introduces a higher duty of care upon data controllers when the processing of data is carried out on their behalf by data processors.[259] The Commissioner (data protection authority) enforces the principles by the serving of enforcement notices.[260] A breach of the data subject's rights will entail a breach of the sixth principle. By enforcing their rights as data subjects, the data subjects therefore also enforce the principles.[261] The data subject may approach the Commissioner or the courts to enforce the obligations of the data controller. Individuals may for example ask the Commissioner for an assessment of any processing by which they believe they are directly affected, and may ask for the assistance of the Commissioner in cases involving the special purposes.[262] An individual who suffers damage or emotional distress by reason of any contravention by a data controller of any of the requirements of the Act is entitled to compensation from the data controller. The court may also make a related order requiring the data controller to rectify, block, erase or destroy personal data, if it is satisfied that the data subject has suffered damage by reason of a contravention by a data controller of the requirements of the Act in circumstances entitling the data subject to compensation, and that there is a substantial risk of further

256(...continued)
controller remains responsible for the security of the processing, even if it uses a data processor to do the processing on its behalf.

257 See ch 3 par 4.2.5.1.

258 DP Act of 1998 s 4(4).

259 See ch 4 par 4.3.4.8.

260 See further ch 4 par 4.3.8.3.

261 Jay & Hamilton *Data protection* 45–46.

262 See ch 4 par 4.3.5.7 and par 4.3.8.

contravention in respect of those data.[263] The Act also creates a number of criminal offences where the data controller does not comply with certain of its obligations.[264]

The WBP also implements the accountability principle by placing the responsibility for ensuring that personal data are processed in accordance with the law and in a proper and careful manner on the data controller, who is called the "responsible party".[265] The WBP gives the data subject remedies in the case of certain decisions (for example in response to a request to correct, supplement, delete or screen data). Where the decision was taken by an administrative body, the aggrieved party has a right to objection (*beswaar*) and appeal (*beroep*). Where the decision was taken by a body other than an administrative body, the aggrieved party may apply to the district court for an appropriate order. Prior to initiating the appeal or court procedures provided for, the party concerned may apply to the CBP (data protection authority) with a request to mediate or give its opinion in the dispute with the responsible party, or may use the dispute arbitration procedure provided for in an approved code of conduct. The WBP also provides remedies for any person who has suffered harm as a consequence of acts which contravene the provisions of the WBP.[266] For harm that does not comprise damage to property, the injured party has the right to fair compensation.[267] Apart from compensation, the courts may also, at the petition of the other parties, impose a ban on conduct by the responsible parties or processors that is in contravention of the provisions laid down by or under the WBP, and order them to take measures to remedy the consequences of such conduct.[268] The WBP furthermore provides for administrative measures of constraint (*bestuursdwang*), administrative fines and penal sanctions to be imposed by the data protection authority.[269] Responsible parties may also be subjected to penal

263 DP Act of 1998 s 14(4) (see ch 4 par 4.3.5.5).

264 See further ch 4 par 4.3.10.

265 WBP a 15.

266 WBP a 49(1).

267 WBP a 49(2).

268 WBP a 50(1).

269 See further ch 5 par ch 5 par 4.3.10.

sanctions in the form of fines or imprisonment.[270]

It is submitted that the accountability principle entails the following:

- Data subjects must be entitled to a judicial remedy, in addition to any administrative remedy, for an infringement of the rights guaranteed by the data protection law.

- Data subjects 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 the data protection laws.

- The data protection law must lay down the sanctions to be imposed in the event of any infringement of its provisions.

It is important that the accountability principle should be incorporated in a data protection law so that the obligations imposed by the law are given teeth and as a consequence are effective.

2.3 Exceptions and exemptions

All the data protection laws studied provide for exceptions to the data protection principles, while certain types of data processing may be totally exempted from the provisions of a particular data protection law.

Broadly speaking, the exceptions and exemptions cover two situations: first, where the risks to the privacy or identity of the data subject are relatively small and second, where other interests (public interests, interests of other parties or those of the data subject himself or herself) override the data subject's rights to privacy and identity. In general, these exceptions and exemptions therefore appear to be justified.

270 WBP a 75.

An example of a situation where a specific processing activity is exempted from the scope of data protection legislation because the risk to the data subject is very small is the provision that the processing of personal data for activities exclusively intended for personal or home use is exempted.[271] A directory of telephone numbers and addresses of friends or acquaintances kept for use at home, should therefore not be considered to be processing of personal data that needs to be regulated by a data protection law.

The rights of the data subject (such as the right to access data, or be informed of certain processing) may also be restricted when such a restriction constitutes a necessary measure to safeguard certain public interests, or to protect the data subject or the interests of others.[272]

An example of where the data subject himself or herself is protected by denying him or her access to personal data is where sensitive medical or psychological information is to be conveyed and the data subject's health or mental state is such that it would be to his or her detriment if the information were conveyed directly to him or her; in other words, it would be to his or her benefit if the information were conveyed indirectly through a health professional.

Third-party information may of course be linked to that of the data subject and in certain situations it might therefore be reasonable to prohibit access by the data subject to such data in order to protect the interests of the third party. An example is where a third party has written a confidential letter of recommendation. In certain cases it might be reasonable to withhold the name of the third party in order to encourage referees to give frank and open evaluations.

It may be permissible in the public interest to restrict the scope of the rights and obligations provided for by the data protection principles in the sense that provision may be made for total or partial

271 Dir 95/46/EC a 3(2); WBP s 2(2)(a).

272 See eg Dir 95/46/EC a 13(1).

exemption from some of those principles.[273] Next, a few of these public interests, with examples from the data protection laws studied, will be discussed.

2.3.1 National security

In the USA, a system of records that is maintained by the CIA may be generally exempted from the Privacy Act's access and amendment provisions, as well as from the provision that the information should be collected directly from the data subject as far as possible. An agency whose system of records consists of classified information or is maintained in connection with providing protective services to the President may also be exempted from several requirements of the Privacy Act, such as the accounting requirement, the access and amendment requirement, the requirement that the notice which must be published in the Federal Register as to the existence of the system of records, should include information about agency procedures and the categories of sources of records in the system, and the requirement that rules should be drawn up to give effect to the provisions of the Act.[274]

The Fair Credit Reporting Act requires that, before taking any adverse action based in whole or in part on a consumer report for employment purposes, the person intending to take such adverse action must furnish the consumer to whom the report relates with a copy of the report and a written description of the consumer's rights under the Fair Credit Reporting Act. However, an exemption from this requirement is made for national security investigations.[275]

In the UK, the broadest exemption that can be claimed by a data controller under the DP Act is where the exemption is necessary for the purpose of safeguarding national security. This exemption applies in respect of all the mechanisms of control under the Act, such as the data protection principles and enforcement by the Data Protection Commissioner. The Act does not define "safeguarding national

273 See Dir 95/46/EC a 13(1); WBP a 43; DP Act of 1998 s 28(1).

274 Ch 2 par 4.2.2.9.

275 Ch 2 par 4.3.2.3.

security" and a certificate of exemption, signed by a Minister of the Crown, is conclusive evidence that the requirements of the exemption have been met.[276]

In the Netherlands, the WBP also provides for exemptions and exceptions in the interests of state security. Exceptions are allowed as regards the principle of compatible use, the general duty to inform all persons, irrespective of their interest, about the processing of personal data, the duty to inform data subjects when their personal data are processed, and the right of data subjects to have access to their personal data.[277] Processing activities that fall under other legislation, such as the Wet op de Inlichtingen en -Veiligheidsdiensten (Intelligence and Security Services Act) are generally exempted from the scope of the WBP.[278]

2.3.2 Defence

In the UK, personal data are exempt from the subject information provisions in any case where the application of those provisions would be likely to prejudice the combat effectiveness of any of the armed forces of the crown.[279]

In the Netherlands, processing by the armed forces can be excluded from the WBP in cases where the Minister of Defence so decides with a view to deploying or making available the armed forces to maintain or promote international legal order. The minister must inform the data protection authority of such a decision.[280]

2.3.3 Public security and safety and criminal investigations

276 See ch 4 par 4.3.6.2.

277 Ch 5 par 4.3.9.

278 Ch 5 par 4.3.3.2.

279 Ch 4 par 4.3.6.3.

280 Ch 5 par 4.3.3.2.

In the USA, law enforcement agencies have immunity from almost every significant restriction in the Privacy Act.[281]

Crime and taxation are primary exemptions in the DPA of the UK. What is involved here is the processing of data for the prevention or detection of crime, the apprehension or prosecution of offenders and the assessment or collection of any tax or duty or of any imposition of a similar nature. Personal data processed for any crime or taxation purpose are exempt in certain instances from the data protection principle that personal data are to be processed fairly and lawfully, the subject access provisions, the subject information provisions and the non-disclosure provisions. These exceptions are always allowed only in so far as the application of those provisions to the data would be likely to prejudice any of the crime and taxation purposes.[282]

In the Dutch WBP, exceptions are allowed for the prevention, detection and pursuit of criminal offences. Where this is necessary in order to trace criminal offences in a particular case, it may be laid down by general administrative order that data processing by the responsible parties who are vested with investigative powers by law is exempt from notification. Compensatory guarantees (*compenserende waarborge*) to protect personal data can be provided in this connection. The processed data may be used only for the purposes expressly stated in the general administrative order.[283] Exemptions are also allowed from the compatible use principle for the detection and pursuit of crime, from the duty to inform all persons about the processing of personal data and the duty to inform data subjects when their personal data are processed, as well as from the right of data subjects to have access to their personal data.[284]

281 See ch 2 par 4.2.2.9.

282 Ch 4 par 4.3.6.2.

283 Ch 5 par 4.3.6.1.

284 Ch 5 par 4.3.9.

2.3.4 Public interest and official authority

According to the Directive, the scope of the rights and obligations created by the principles regarding data quality and providing information to the data subject may be restricted where 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. An example here would be investigations of breaches of ethics for regulated professions.[285]

2.3.5 Important economic or financial interests of the state

The UK DPA provides for an exemption from the subject information provisions[286] if required for the purpose of safeguarding an important economic or financial interest of the UK, subject to an order by the Secretary of State clarifying when and in what circumstances such an exemption is available.[287]

The WBP allows exceptions with regard to the principle of compatible use and the general duty to inform all persons, irrespective of their interest, about the processing of personal data for the sake of important economic and financial interests of the state and other public bodies.[288]

285 See ch 3 par 4.2.4.1 and par 4.2.4.5.

286 These provisions are equivalent to the fair processing code, which requires data controllers to inform data subjects of various matters, and the subject access provisions (see ch 4 par 4.3.6.1).

287 Ch 4 par 4.3.6.3.

288 Ch 5 par 4.3.6.2 and 4.3.7.2.

2.3.6 Public health, social protection, scientific research, government statistics

Exceptions are also made for substantial public interests such as public health[289] and social protection, scientific research, and government statistics. A proviso is usually added to these last types of exceptions, namely that "suitable safeguards" must be introduced.[290] This would mean for example that in the case of statistical research the anonymity of the data should be ensured and that in the case of a person processing medical data, the person doing the processing should be subject to a duty of confidentiality.

2.3.7 Journalistic or artistic purposes

Exceptions to the data protection principles are also allowed where personal data are processed solely for journalistic purposes or the purpose of artistic or literary expression, if such exceptions are necessary to reconcile the right to privacy with the rules governing freedom of expression.[291]

2.3.8 Sound and image data

As a general rule, personal information in sound and image data (for example closed circuit television recordings) are not excluded, but additional requirements are imposed, for example that such data must form part of a structured set of data that can be accessed according to specific criteria relating to individuals, such as name or identification number.[292]

In conclusion, it is evident that exceptions to the data protection principles are necessary in order to

289 Eg, for purposes of preventive medicine, medical diagnosis, provision of care or treatment or the management of health-care services (see Dir 95/46/EC a 8(3)).

290 Dir 95/46/EC a 8(4). See also ch 4 par 4.3.6.2 and ch 5 par 4.3.9.

291 Dir 95/46/EC a 9. See also ch 3 par 4.2.4.4, ch 4 par 4.3.6.2; ch 5 par 4.3.3.2.

292 See eg the Directive's provisions in this regard (ch 3 par 4.2.3).

achieve a proper balance between the rights that data protection legislation aims to protect and the rights and interests of third parties and the public.

2.4 Defences

Most of the data protection statutes provide for civil remedies for a contravention of the provisions of the statute, but at the same time offer the data controller or data processor certain defences against liability.

Under the Privacy Act, for example, an individual may bring a civil action against an agency on several grounds,[293] but actual damages will only be awarded if the court decides that the agency acted intentionally or wilfully.[294] Negligence is not sufficient for liability; so even if an agency acted unreasonably it will not be held liable.

In the case of the Fair Credit Reporting Act, a consumer may institute an action against an agency or user who willfully, knowingly or negligently fails to comply with any requirement of the Act. In this case the agency will therefore not be held liable as long as it acted in a reasonable manner.[295]

The EU data protection Directive provides that individuals are entitled to a judicial remedy for an infringement of the rights guaranteed by the data protection legislation, but controllers may be exempted from this liability if they prove that they are not responsible for the event giving rise to the damage. The absence of a causal link between their conduct and the event that gave rise to damage will therefore exclude liability.[296] Fault on the part of the data subject or *vis major* is a defence.[297] It would therefore

293 See ch 2 par 4.2.2.13.

294 5 USC s 552a(g)(4).

295 See ch 2 par 4.3.2.11.

296 Dir 95/46/EC a 23(2) (see ch 3 par 4.2.5.1).

297 Dir 95/46/EC recitals par (55).

seem that the Directive makes provision for strict liability or liability without fault.[298]

The Dutch WBP implements the Directive by providing remedies for persons who have suffered harm as a consequence of acts which contravene the provisions of the Act.[299] For harm that does not comprise damage to property, the injured party has the right to fair compensation.[300] In general, the responsible party (that is the data controller) is liable for such loss or harm, but where this was incurred as a result of the action of a processor, the processor will be liable for his or her part of the damage.[301] The controller nevertheless also remain liable, but has a right of recourse against the processor.[302] The data controller and processor may be exempted wholly or partially from their liability where they can prove that the harm cannot be attributed to them.[303] The burden of proving that they are not liable rests with them.[304]

The UK DP Act provides that an individual who suffers damage as a result of any contravention by a data controller of any of the requirements of the Act is entitled to compensation from the data controller for that damage.[305] It is a defence for a data controller against such proceedings to prove that he or she had taken reasonable care in the circumstances to comply with the requirement in question.[306]

298 Also see fn 304.

299 WBP s 49 (see ch 5 par 4.3.10.1).

300 WBP s 49(2).

301 WBP s 49(3).

302 WBP *Memorie van toelichting* 176.

303 WBP s 49(4).

304 The first data protection act in the Netherlands, the WPR, made provision for risk-liability, but according to the WBP *Memorie van toelichting* 176 this has been watered down in the WBP because the Directive (a 23(2)) allows for exemption from liability. Also see Holvast 1998 (1) *Priv & Inf* 4, 6. It is submitted, however, that this nevertheless remains a form of strict liability, because *vis major* is a generally recognised defence in the case of strict liability (see Neethling, Potgieter & Visser *Delict* 365).

305 DP Act of 1998 s 13(1) (see ch 4 par 4.3.5.5).

306 DP Act of 1998 s 13(3).

It is submitted that data controllers should be strictly liable. *Vis major*, fault on the part of the data subject, and the fact that the data controller took all reasonable steps to comply with the data protection principles, should however be defences against such liability.[307]

2.5 Differences in implementation

As stated previously, the areas in which data protection laws differ the most are the mechanisms employed to enforce data protection and in the scope of the legislation.

2.5.1 Models of data protection

EPIC, in an international survey of data protection laws, identify four models of data protection.[308] These models may be contradictory or supplementary – it all depends on how they are applied. EPIC found that in most countries included in its survey several models are used simultaneously. In fact, in the countries where privacy is protected most effectively, all the models are used in combination.

2.5.1.1 Comprehensive laws

A general law governs the processing of personal information by both the public and the private sectors. An oversight body ensures compliance. According to EPIC this is the preferred model for most countries adopting data protection legislation.[309] This is the model adopted by the EU Directive and implemented by the UK and the Netherlands.[310]

---

307 See text to fn 296, fn 297, fn 298 and fn 306 and above. See ch 7 par 2.3.2.3 for a discussion of the defence of "impossibility".

308 EPIC *Privacy and human rights* 3 *et seq*.

309 EPIC *Privacy and human rights* 4.

310 EPIC *Privacy and human rights* 4 points out that there is a variation on these laws, described as a co-regulatory model. Canada and Australia have adopted this model, in which industry develops and enforces the rules for the protection of privacy and the data protection agency oversees the enforcement.

2.5.1.2 Sectoral laws

In this model countries do not adopt a general data protection law, but adopt different laws for different sectors. The USA is a prime example of such a system, with laws at the federal level for *inter alia* government agencies, educational institutions, banks, newsrooms, departments of motor vehicles, medical institutions, cable television providers, electronic communications providers, video rental companies, telecommunication providers, and credit companies. The drawbacks of such a model are that new legislation must be introduced with each new technology that poses a threat to privacy and that there is no single oversight body that provides effective control of processing of personal data.[311] Furthermore, it is difficult for data subjects to know and understand their rights in relation to their personal data when such rights differ from sector to sector.

Sectoral laws can also be adopted to supplement a general data protection law. In the Netherlands for example, in addition to the WBP, there are also laws for police files, municipal records, intelligence and security services records and medical information.[312] Such laws can provide more detailed protection in areas where sensitive personal information is processed.

2.5.1.3 Self-regulation

In theory data protection can be achieved through various forms of self regulation, in which companies and industrial bodies establish codes of conduct and then engage in self-enforcement or self-regulation.[313] In the USA, many companies, especially those that have adopted the OECD Guidelines[314] have implemented this model. However, these efforts proved to be "disappointing, with little evidence

311 EPIC *Privacy and human rights* 4. See further Neethling *Persoonlikheidsreg* 327–328.

312 See ch 5 par 4.1.

313 See also Bennett *Regulating privacy* 155 *et seq*.

314 See ch 3 par 2.

that the aims of the codes are regularly fulfilled".[315] This model has also been adopted in the Safe Harbor agreement between the USA and the EU.[316] A major problem with this model is that it provides weak protection and lacks enforcement mechanisms.[317]

2.5.1.4 Personal self-protection through technology

This is not really a model of data protection, but describes a situation where data subjects take responsibility for their privacy and use technology when interacting on-line with potential data controllers. This technology (referred to as "PETS"[318]) includes the use of encryption,[319] anonymous remailers,[320] proxy servers[321] and digital cash.[322] Although data subjects should be encouraged to take responsibility for protecting their privacy, this is not the solution for data protection in the long run. It is also only of use in an on-line environment.

2.5.2 Enforcement mechanisms

The most notable difference between the USA on the one hand, and the European countries on the

315 EPIC *Privacy and human rights* 4.

316 See ch 2 par 5.

317 Bennett *Regulating privacy* 156 points out that "[v]oluntary control does not guarantee ... that personal data protection interests will prevail when confronted with the quest for efficiency and cost-effectiveness".

318 PETS is the acronym for Privacy Enhancing Techniques.

319 Encryption entails the process of converting data in a message into a secret code prior to transmission via public telecommunication channels, to make it unreadable to all but the authorised recipient who can convert the encoded message back into the original information.

320 An anonymous remailer is a server that receives messages with embedded instructions on where to send them next and forwards them without revealing where they came from.

321 A proxy server is a system that caches items from other servers to speed up access. On the WWW, a proxy server first attempts to find data locally, and if the data are not there, it fetches them from the remote server where the data reside permanently. Apart from providing quicker downloads for users, it also increases server security, because it allows direct Internet access from behind a firewall.

322 Digital cash is a generic term that describes the electronic cash or digital currency used in cyberspace. See further EPIC *Privacy and human rights* 64 *et seq*.

other is the manner in which the data protection principles are enforced.

2.5.2.1 Enforcement by data subject

Every data protection regime that permits data subjects the right to participate in data protection[323] and to have recourse to the courts in effect employs a model of enforcement by the data subject. In the USA, however, enforcement by the data subject is a major part of the enforcement system. There is no general data protection authority to oversee the implementation of the Privacy Act[324] – the chosen method of implementing the Privacy Act has been described as "voluntary compliance and self-help".[325] In other words, it is up to the agencies themselves to comply with the Act and an individual has to enforce his or her rights under the Act through the courts. As Bennett correctly opined, the drawback of such a system is that it is "dependent on an activist and litigious citizenry that is concerned about privacy and willing to assert its rights either directly with the record-keeping organization or indirectly through the courts".[326]

The lack of an oversight body is the major weakness in the Privacy Act. Flaherty,[327] after a comparative study of the implementation of data protection laws in Germany, Sweden, France, Canada and the USA, concluded that the USA "carries out data protection differently than other countries, and on the whole does it less well, because of the lack of an oversight agency".

The Fair Credit Reporting Act also relies on consumers (the data subjects) to enforce the Act through

323 By giving data subjects eg the right to have access to personal data and the right to request correction of incorrect, irrelevant or misleading data.

324 Instead, oversight takes place on different levels, namely by the head of the agency, the Office of Management and Budget (OMB), the US President, Congress and the courts. A major dispute when enacting the Privacy Act was how the Act was to be implemented (see ch 2 par 4.2.1.5).

325 Bennett *Regulating privacy* 170. Another apt description is that of Schwartz 1991 *Am J Comp L* 618, 619 who calls the American approach to oversight of data protection the "dispersed responsibility model".

326 Bennett *Regulating privacy* 157.

327 Flaherty *Surveillance societies* 305. He therefore concluded that it is not enough to pass data protection legislation but that an agency charged with implementation is essential to make the law work in practice.

the courts. Administrative enforcement is entrusted to the Federal Trade Commission (FTC), which can enforce the Act in terms of its powers under the Federal Trade Commission Act.[328]

2.5.2.2 Enforcement by data protection authority

With this method of enforcement a data protection authority is established to act as an intermediary between the data subjects and data controllers. In early legislation the authority sometimes only had an ombudsman function, but more recent legislation grants the authority effective powers of oversight and enforcement. The authority can oversee data processing by requiring the data controllers to licence their computers with the authority,[329] to register with the authority as a data controller,[330] or to notify the authority that it is processing data.

The EU Directive does not prescribe in any detail the regulatory scheme that must be followed 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 by the different sectors of the data processing industry. In other 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.[331] The Directive also prescribes that the independent supervisory body is obliged to have effective powers of investigation and the power to engage in legal proceedings where the national data protection legislation

328 See ch 2 par 4.3.2.13.

329 This method of supervision was employed by Sweden (see Bennett *Regulating privacy* 161). This type of supervision only works for computerised systems and also only where no computerised system is already in place. In its purest sense, this method entails that no system may be started before it has been licensed. Every piece of data that goes into the system has to be cleared before the system is put in operation. None of the countries researched for this thesis employed this method.

330 The 1984 UK Data Protection Act implemented oversight be means of mandatory registration. This was replaced by a notification system under the 1998 Act. The large-scale availability of personal computers since the 1980s has resulted in registration no longer being an attainable aim. By the 1990s the registration system came to be considered to be burdensome, bureaucratic and unnecessarily detailed.

331 See ch 3 par 4.2.5.

has been violated.[332] The Directive further provides that member states should encourage the drawing up of codes of conduct.

The data protection legislation of the Netherlands and the UK essentially follows the Directive's provisions, but since the Directive does allow member countries some leeway in the way they implement its provisions, it is worthwhile to briefly compare implementation in the two countries.

In the UK the Office of the Information Commissioner is the independent body responsible for enforcing the principles of the DP Act, with the option of appeal to a Data Protection Tribunal.[333] Data controllers are obliged to notify the Commissioner of any processing of personal data that will take place, unless that type of processing is exempted from notification.[334] The primary purpose of notification is to promote transparency where data processing is taking place.

The DP Act also enables the Secretary of State to provide for the appointment of data protection supervisors by the data controllers, in which case the notification procedure may be simplified.[335] The Commissioner must keep a register of all notifications, which register must be open for inspection by members of the public.[336]

Certain categories of processing, to be determined by the Secretary of State, are also subject to a preliminary assessment by the Commissioner.[337] The Commissioner may enforce the Act by serving information notices and enforcement notices.[338] The Commissioner is also empowered to draw up codes

332 See ch 3 par 4.2.5.2.

333 See ch 4 par 4.3.9.

334 See ch 4 par 4.3.7.

335 See ch 4 par 4.3.7.3

336 See ch 4 par 4.3.7.6.

337 See ch 4 par 4.3.7.7.

338 See ch 4 par 4.3.8.2 and par 4.3.8.3.

of conduct for guidance and to consider codes of conduct presented by trade associations.[339] An individual who suffers damage by reason of a contravention of the Act by the controller is entitled to compensation for such damage and accompanying distress.[340] The DP Act also creates offences which can be tried in the civil courts.[341]

In the Netherlands the independent supervisory authority which has to oversee the processing of personal data and ensure that it takes place in accordance with the WBP is known as the College Bescherming Persoonsgegevens (CBP).[342] Data controllers are obliged to notify the CBP of any intended processing of personal data unless that type of processing is exempted from notification.[343] The WBP allows controllers to appoint data protection officers.[344] The CBP, or a particular data protection officer, must keep a register of all notifications made to them, which register must be open for inspection free of charge.[345] In three specific instances, the CBP has the authority to institute a prior investigation on processing activities reported to it.[346] The members and officials of the CBP may enforce the Act by using administrative measures of constraint.[347] The CBP must consider a code of conduct drawn up by an organisation operating in a specific sector and, if this code of conduct reflects the nature of the sector and correctly applies the data protection principles, the CBP must make a declaration to that effect and publish the code of conduct in the *Government Gazette*.[348] An individual has several remedies available, such as appeal and objection where an adverse decision has been taken by an

339 See ch 4 par 4.3.9.1.

340 See ch 4 par 4.3.5.5.

341 See ch 4 par 4.3.10.

342 See ch 5 par 4.3.11.1.

343 See ch 5 par 4.3.6.1.

344 See ch 5 par 4.3.11.2.

345 See ch 5 par 4.3.6.2.

346 See ch 5 par 4.3.6.3.

347 See ch 5 par 4.3.11.1.

348 See ch 5 par 4.3.5.

administrative body, or appeal to a court against a decision taken by a body other than an administrative body. An individual who has suffered damage by reason of a contravention of the Act may apply to the court for compensation by either the controllers or the processors, and such compensation would include fair compensation for harm that does not comprise damage to property.[349] The WBP also provides for administrative measures of constraint and penal sanctions.[350]

In conclusion, it is evident that successful modern data protection laws provide for an independent data protection authority with the necessary powers to supervise compliance with the basic data protection principles. Such a body has investigative powers and powers to engage in legal proceedings where the data protection legislation has been violated. One of its functions is to encourage and assist representative bodies in drawing up codes of conduct for their sectors[351]. The individual also has rights of enforcement independent of the data protection authority, such as the right to object or appeal to a court against a decision taken by a data controller. An individual who has suffered damage by reason of a contravention of the data protection law is usually also entitled to compensation by either the data controllers or the data processors.

2.5.3 Scope of legislation

The main differences that arise in the scope of legislation relate to –

- the scope of the sector covered: the public or private sector or both

349 See ch 5 par 4.3.10.1.

350 See ch 5 par 4.3.10.2.

351 Schwartz 1995 *Iowa L R* 471, 492–494 highlights three important institutional roles that a data protection authority can fulfil: First, the data protection authority develops expertise in an area that is subject to technological developments, which expertise can be made available to government, business, and private citizens. Second, it develops and monitors international agreements and foreign laws affecting data imports and exports. Third, through its knowledge of technological developments and oversight of international legal developments, it can be a focal point for an ongoing national and international debate regarding the application of information processing devices.

- the range of data subjects: that is, only natural persons (individuals) or also juristic persons;[352] all persons in the country or only citizens; only living individuals or also deceased persons

- whether the data should be processed automatically in order to fall within the scope of the law, or whether manually processed data are also included

The United States does not have an omnibus law so it is to be expected that the scope of its legislation in this area will be varied. For example, the Privacy Act regulates only the public sector (at federal level) and only gives rights to US citizens or lawfully admitted aliens.[353] The Fair Credit Reporting Act applies only to consumer reporting agencies and protects only individuals.[354]

The OECD Guidelines apply to the private and public sectors, as well as to manually and automatically processed data. But the Guidelines recognise only individuals as data subjects.[355] The Council of Europe Convention applies to automated processing of personal data on an individual in the private and public sectors. However, parties to the Convention may extend the scope of their legislation to include groups of persons, with or without legal personality, as data subjects. They may also include manually processed files.[356]

The European Union Directive applies equally to processing in the private and public sectors and to processing by automatic and nonautomatic means. However, in the case of nonautomatic processing the personal data must form part of a filing system that allows for access according to specific criteria.

352 None of the countries studied include juristic persons so that no comparative conclusion can be drawn on this topic as yet. A more detailed analysis of this issue is undertaken in ch 7 par 2.5.2.

353 See ch 2 par 4.2.2.3.

354 See ch 2 par 4.3.2.2.

355 See ch 3 par 2.2.4.

356 See ch 3 par 3.2.3.

Only natural persons can be data subjects.[357]

As might be expected, the UK's DP Act[358] and the Netherlands' WBP[359] in essence follow the European Union Directive's provisions. There was a difference of opinion as to whether the term "individual" as used in the Directive also includes a deceased person. English commentators argued affirmatively, whereas Dutch commentators were of the opinion that it only includes living persons. The UK Act now explicitly refers to "living individuals".[360] The Dutch Act only refers to natural persons, which would probably be interpreted as referring to living individuals only.[361]

In conclusion it can be said that the majority of the most recent acts or instruments extend data protection to living individuals in regard to automatically or manually processed data in both the public and private sectors. As will be demonstrated later,[362] a good case can be made out for including juristic persons under the scope of the data protection laws.

2.5.4 Regulatory trends

In this thesis, the different laws and other data protection instruments were discussed in a more or less chronological order. As pointed out by Bygave, "[m]oving from the oldest of the data protection instruments to the youngest, we can discern certain regulatory trends".[363] In concurrence with

357 See ch 3 par 4.2.3.

358 See ch 4 par 4.3.3.1.

359 See ch 5 par 4.3.3.

360 See ch 4 par 4.3.3.1.

361 See ch 5 par 4.3.3.1.

362 See ch 7 par 2.5.2.

363 "In data protection discourse, it is popular to categorise these trends as in terms of 'generations'; ie, one generates between , ia, 'first-', 'second-', and 'third-generation' data protection laws" (Bygrave *Data protection law* 87–88).

Bygrave,[364] the following trends may be mentioned:

- a trend towards more detailed provisions and requirements[365]
- an increasing attempt to enforce compliance with data protection principles by laying down procedural requirements[366]
- a shift and consolidation in regulatory focus[367]
- a shift away from comprehensive licensing regimes to a simpler system of notification (or registration at the most) of data-processing operations[368]

3 SUMMARY

In this chapter it was concluded that data protection legislation is absolutely necessary to protect the rights to privacy and identity of individuals, who can no longer control the use made of their personal

364 Bygrave *Data protection law* 88.

365 Bygrave refers to this as "increasing regulatory density" (Bygrave *Data protection law* 88).

366 Compare, eg, the provisions in the OECD Guidelines and the Convention on "fair" processing of personal data with the more elaborate provisions of the Directive (see ch 3 par 2.2.5; par 3.2.4; and par 4.2.4).

367 Note eg the shift from regulating the "collection, use and disseminating" of personal data to the "processing" of personal data; also the increasing focus on regulating "personal data" *per se* rather than "personal data files". Also noteworthy is the shift to include manually processed data in addition to automated data processing and the increasing use of sectoral codes of practice.

368 According to Bygrave *Data protection law* 88, "this is a development in which anticipatory control by data protection authorities gives way to (though is not necessarily extinguished by) more reactive control on the part of such authorities. This development is offset by enhancement (at least on paper) of the opportunities for participatory control: data subjects' access rights are supplemented by more extensive notification duties for data controllers, and there is greater readiness to make the consent of data subjects a prerequisite for certain kinds of data processing. Certainly, this gives individuals more room to determine for themselves the manner and extent to which data on them are processed, though it does not necessarily mean that individuals will act to limit such processing or that such processing will decrease. Moreover, data controllers will often be able to avoid the consent rule because of the existence of broadly drawn, alternative requirements for the data processing in question".

information. International expectations also mean that countries without data protection legislation will have to adopt such legislation if they want to remain part of the international information community. Despite differences in language, legal traditions and cultural and social values, there has been a broad measure of agreement on the basic content and rules that should be embodied in data protection legislation. It is essential that all the data protection principles should be given effect to in any data protection law, and that an oversight body should be established.