Chapter 5
Netherlands

Contents

1 INTRODUCTION

In the Netherlands, as in many other countries, fear of the use of computers to collect information on individuals, especially during a planned national census, started the discussion on data protection in the late sixties that resulted in the adoption of data protection legislation.

Today the Netherlands is part of the European Union, and must therefore comply with the European Union Directive on data protection which compels member countries to adopt data protection legislation that adheres to the standards prescribed therein.[1]

Before discussing the legislation that was adopted pursuant to the Directive, the protection of privacy

1 Dir 95/46/EC. See ch 3 par 4. Hereafter referred to as "the Directive".

in Dutch private and constitutional law will briefly be referred to.[2]

2 PROTECTION OF PRIVACY IN PRIVATE LAW

2.1 Concept of privacy

According to Verhey,[3] the first discussion of the concept of privacy in Dutch legal literature dates from 1965.[4] Since then legal writers in the Netherlands[5] have wrestled with, and argued about, the precise content and meaning of privacy.[6] Different terms (namely privacy, *privé-levenssfeer, persoonlijk leven, privé-sfeer, persoonlijke levenssfeer, persoonlijke vrijheid, privé-leven*[7]) are used to refer to privacy. Although writers do not agree on the definition or content of the right to privacy, the issue can be simplified by stating that privacy is generally seen as relating to the intimacy of the home and other physical places to which one would like to retreat from the public eye, but that it also refers to a nonphysical sphere, the extent of which is determined by individuals for themselves.[8] Because of the influence of technology on the collection of information on individuals, yet another privacy concept has

2 These discussions should merely be seen as brief introductions, since the two topics fall outside the scope of this thesis.

3 Verhey *Horizontale werking van grondrechten* 192.

4 By De Brauw and Van Veen *Preadviesen NJV* (Nederlandse Juristenvereniging) (1965) (quoted by Verhey *Horizontale werking van grondrechten* 192 fn 3). The seminal article by Warren and Brandeis 1890 *Harvard LR* 193 is also referred to in Dutch legal literature as the foundation of the development of the right to privacy (see Verhey *Horizontale werking van grondrechten* 192; Sentrop *Privacy-bescherming* 11–12).

5 See eg the following dissertations quoted by Verhey *Horizontale werking van grondrechten* 192: Aubel *Persoon en pers* (1968); De Graaf *Persoonlijkheid, privé-leven, persoonsgegevens* (1977); Holvast *Op weg naar een risicolose maatschappij? De vrijheid van de mens in het informatietijdperk (*1986).

6 See eg Kuitenbrouwer "Privacy" 7 ("[H]et begrip [privacy] valt wel aan te duiden, maar nauwelijks te definiëren"); Sentrop *Privacy-bescherming* 11 ("Het begrip 'privacy' ontrek zich .. aan een scherp omlijnde definiëring"); Nabben & Van de Luytgaarden *De ultieme vrijheid* 66 "[Er] bestaat ... zowel in de wetgewing als in de rechtspraak en literatuur geen duidelijkheid over de inhoud en reikwijdte van het recht op privacy").

7 Nabben & van de Luytgaarden *De ultieme vrijheid* 67.

8 De Brauw and Van Veen Preadviesen *NJV* 1965 10 (see fn 4) defines privacy from this broader perspective as "het geheel der omstandigheden waaronder de individu bepaalde gedragingen en uitingen aan de waarnemingen van de gemeenschap wil ontrekken".

developed, a concept referred to as *informationele privacy* (informational privacy).[9]

Holvast[10] follows Westin[11] when he argues that in the modern privacy concept two fundamental rights should be distinguished:

- the right to selective interaction (*contactlegging*) with the right to be let alone as the most extreme form (relational privacy)

- the right to selective disclosures (informational privacy)[12]

2.2 Infringement of privacy as a wrongful act (delict)

In Dutch law, the general action arising from a wrongful act (*onrechmatige daadsactie*) is to be found in article 162 of Book 6 of the new Civil Code (Burgerlijke Wetboek (BW)). In terms of article162(1), a person who commits a delict against another, for which that person can be held accountable, must compensate the other person for the damage[13] he or she has suffered. Article 162(2) prescribes that conduct is considered to be unlawful if, in the absence of a ground of justification, the conduct (which may be a commission or an omission) is in conflict with a legal obligation,[14] or infringes a subjective

9 Following Westin *Privacy and freedom* 7 (see Verhey *Horizontale werking van grondrechten* 194).

10 Holvast *Op weg naar een risicolose maatschappij? De vrijheid van de mens in het informatietijdperk* (1986) 25 (quoted by Verhey *Horizontale werking van grondrechten* 194). Also see Frankena "Bescherming van privacy en persoonsgegevens" 324.

11 Westin *Privacy and freedom* 7.

12 See also Schuijt *Onrechtmatige daad VII* fn 101.

13 Compensation for immaterial damage pursuant to infringement of the personality takes place in terms of Book 6 a 106(1)(a) of the Civil Code (see Nieuwenhuis et al *Nieuw burgerlijk wetboek* 523–525).

14 This is interpreted as referring to a *wettelijke plig*, ie a duty that arises eg from legislation, a treaty with direct effect, or general administrative orders. An example would be where a criminal provision is infringed. Such infringement also results in an action for unlawful conduct (Asser-Hartkamp III (*Verbintenissenrecht*) 38).

right, or is against what is considered by the unwritten law to be generally acceptable.[15]

The action arising from an unlawful act can therefore be used where privacy has been infringed, because the right to privacy is a subjective right,[16] more specifically a personality right.[17] Furthermore, where a legal provision aimed at protecting an individual's privacy[18] is transgressed, this transgression also results in an action in delict.[19]

3 PROTECTION OF PRIVACY UNDER CONSTITUTIONAL LAW[20]

15 See Asser-Hartkamp III (*Verbintenissenrecht*) 40; Nieuwenhuis et al *Nieuw burgerlijk wetboek* 587–588.

16 See Asser-Hartkamp III (*Verbintenissenrecht*) 40; Nabben & Van de Luytgaarden *De ultieme vrijheid* 48 *et seq*. See also Sentrop *Privacy-bescherming* 161 (note that he refers to a 1401 of the old Civil Code). Nabben & van de Luytgaarden *De ultieme vrijheid* 48 point out that although it is accepted that civil law recognises an infringement of privacy as "a schade toebrengend feit" the courts are nevertheless "zeer spaarzaam met de erkenning van het recht op privacy als grond voor een actie uit onrectmatige daad". See Schuijt *Onrechtmatige daad* VII fn 101–114 for relevant case law.

17 The term *persoonlikheidsrecht* cannot be found in Dutch legislation, but it is used in case law and legal literature. However, it has not precisely been established what the term means. See also Frankena "Bescherming van privacy en persoonsgegevens" 324.

18 See eg the Auteurswet (*Stb* 1912 308) (Copyright Act of 1912) which provides that a person may prohibit publication of a photograph of himself or herself, and thus protects an aspect of his or her privacy. See Nabben & Van de Luytgaarden *De ultieme vrijheid* 49; Schuijt *Onrechtmatige daad* VII n 121 *et seq*. Criminal law also plays an important role in the Netherlands in protecting aspects of privacy (see Nabben & Van de Luytgaarden *De ultieme vrijheid* 45–48; Schuijt *Onrechtmatige daad* VII n 5).

19 See eg HR 9 January 1987, AB 1987, 231 and NJ 1987, 928 (the *Edamse Bijstand* case) where it was held that infringement of a constitutional right to privacy can result in an action based on unlawful conduct (also see fn 31). In this case, a woman claimed that in terms of a 1401 (old) BW her neighbour, who was also working as a deputy-director of the local GSD (Gemeentelijke Sociale Dienst) should be prohibited from keeping notes on her conduct and giving this information to third parties. The woman was denied assistance in terms of the Algemene Bijstandswet (*Stb* 1960 284). (The Act imposes a duty on the government to give assistance to citizens of the Netherlands living in the Netherlands who cannot provide for themselves.) When she was given access to her file at the GSD, she realised that assistance had been denied because of the information given to the GSD by her neighbour. The neighbour had observed her over a period of time and had made regular reports on her private life to the GSD. He reported that she was living with a man, and thus formed an "economic unit" with someone who had an income. In terms of the Act, she could not receive assistance if this was indeed the case. However, on review her claim for assistance was upheld. The Hoge Raad (HR) held that the neighbour had infringed the woman's right to respect for her private life. However, this does not mean that the infringement was unlawful, because a ground of justification could have been present. The case was referred back to the lower court which had to decide on the basis of the facts of the case whether a ground of justification was present.

20 For a detailed discussion of the right to privacy as a *grondrecht* (constitutional right), see the thesis by (continued...)

The Dutch Constitution was amended in 1983 to include article 10 in which privacy (*persoonlijke levenssfeer*) is explicitly protected.[21] Article 10(1) provides that everyone has a right to privacy whereas articles 10(2) and 10(3) refer to the protection of any personal information that has been recorded.[22] These articles instructed the legislator to adopt legislation to protect privacy in recorded personal information.[23] This resulted in several pieces of legislation containing data protection provisions.[24]

Other articles in the Constitution also result in the protection of aspects of privacy and should be read with article 10.[25] Article 11 protects the integrity of an individual's body, article 12 the sanctity of the individual's house and article 13 the privacy of letters and telephone conversations.[26]

20(...continued)
Verhey *Horizontale werking van grondrechten*. See also Overkleeft-Verburg*De Wet Persoonsregistraties* 21–33.

21 On the revision of the Dutch Constitution, see Overkleeft-Verburg *De Wet Persoonsregistraties* 50–51.

22 The Dutch Constitution a 10 states:

> 1. Ieder heeft, behoudens bij of krachtens de wet stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
> 2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
> 3. De wet stelt regels inzake aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

(See Sentrop *Privacy-bescherming* 161.)

23 See De Graaf "Wet Persoonsregistraties" 362.

24 The Wet Op De Inlichtingen- en Veiligheidsdiensten *(Stb* 1987 635), Wet Persoonsregistraties (*Stb* 1988 665), Wet op Politieregisters (*Stb* 1990 414), Wet Gemeentelijke Basisadministratie Persoonsgegevens (*Stb* 1994 494) and Wet Geneeskundige Behandelingsovereenkomst (*Stb* 1994 838) were all adopted pursuant to this requirement (see par 4.1 and see Nabben & Van de Luytgaarden *De ultieme vrijheid* 28). Also see Overkleeft-Verburg *De Wet Persoonsregistraties* 26.

25 See Verhey *Horizontale werking van grondrechten* 198; Nabben & Van de Luytgaarden *De ultieme vrijheid* 25–26; Kuitenbrouwer et al *Drieluik privacybescherming* 50.

26 EPIC *Privacy and human rights* 272 reports that in May 2000, "the government-appointed commission for 'Constitutional rights in the digital age' presented proposals for changes to the Dutch constitution. The commission was set up after confusion about the legal status of e-mail under the constitutionally protected privacy of letters. The commission's task was to investigate if existing constitutional rights should be made more technology-independent and if new rights should be introduced. According to this proposal article 10 will be expanded to the right of persons to be informed about the origin of data recorded about them and (continued...)

Article 8 of the European Convention on Human Rights also protects the right to private life. This Convention has been ratified and incorporated into national law by the Netherlands, and thus forms part of the law of the Netherlands.[27] In 1987 the Hoge Raad held in the *Edamse bijstand* case[28] that the right to privacy as protected by article 8 of the European Convention on Human Rights[29] is horizontally applicable (that is, it is applicable between individuals).[30] An infringement of the constitutionally protected right to privacy could therefore also result in an unlawful act (a delict).[31]

In conclusion, it can be said that "[t]he right of privacy traditionally is strongly integrated in the Dutch system of law, in the Constitution, written and unwritten secrecy pledges, specific laws and judicial decisions; it is sanctioned by criminal law, civil law and disciplinary rules. From the viewpoint of norms, the system has been rather effective and also very flexible, although fragmented with a heavy emphasis on casuistry".[32]

4 PROTECTION OF DATA PRIVACY BY MEANS OF LEGISLATION:

26(...continued)
the right to correct that data. Article 13 would be made technology-independent and would give the right to confidential communications. Breaches of this right could only be authorised by a judge or a minister. The discussion about possible changes is still ongoing".

27 See Harris, O'Boyle & Warbrick *European Convention on Human Rights* 24.

28 HR 9 January 1987, AB 1987, 231 and NJ 1987, 928. See fn 19 for a discussion of the case.

29 When the facts of the case under discussion occurred, a 10 of the Dutch Constitution was not in operation yet (see Overkleeft-Verburg *De Wet Persoonsregistraties* 65 fn 15).

30 For a detailed discussion of the horizontal applicability of the right to privacy as a constitutional right, see the thesis by Verhey *Horizontale werking van grondrechten.*

31 See HR 9 January 1987, AB 1987, 231 and NJ 1987, 928 par 4.4:
> Vooropgesteld moet worden dat, ook voor de periode waarin zich de feiten van de onderhavige zaak hebben afgespeeld, een recht op eerbiediging van de persoonlijke levenssfeer moete worden aanvaard, dat aansluit bij vergelijkbare ontwikkelingen in andere landen en dat naar zijn inhoud mede wordt bepaald door art. 8 EVRM, [Europees Verdrag betreffende de Rechten van de Mens en de fundamentele vrijheden] waarvan moet worden aangenomen, dat het ook werking heeft tussen de burgers onderling. Een inbreuk op dit recht levert in beginsel een onrechtmatige daad op in de zin van art. 1401 BW."

(A 1401(old) BW has been replaced by a 162 in the new BW). Also see fn 19.

32 Overkleeft-Verburg *De Wet Persoonsregistraties* 699.

WET BESCHERMING PERSOONSGEGEVENS OF 2000

4.1 Introduction

The Wet Bescherming Persoonsgegevens (WBP) (Personal Data Protection Act) of 2000 is the general data protection legislation in the Netherlands. The WBP replaces the Wet Persoonsregistraties (WPR) (Registration of Persons Act) of 1989.[33] However, there is also other legislation that protect privacy in specific types of data files, for example the Wet Politieregisters (Police Files Act), the Wet Gemeentelijke Basisadministratie Persoonsgegevens (Municipal Database (Personal Records) Act), the Wet op de Inlichtingen- en Veiligheidsdiensten (Intelligence and Security Services Act)[34] and the Wet Geneeskundige Behandelingsovereenkomst (Medical Treatment and Information Act).[35] This thesis focuses on the WBP, but reference will be made to the other sectoral legislation where this is relevant.

4.2 Background and legislative history of WBP[36]

4.2.1 Wet Persoonsregistraties

In the Netherlands, the history of privacy legislation began with the general census of 1971.[37] The census was planned in response to a request by the United Nations, the European Commission and Benelux that countries should conduct a census in or around 1970.[38] For the first time census forms were used that could be processed by computer (punch cards). Although the idea was that the forms

33 WBP a 81.

34 For references regarding these Acts, see fn 24.

35 *Stb* 1994 838.

36 This paragraph relies on Nugter *Transborder flow of personal data* 145–147 and Berkvens & Prins "Van WPR naar WBP" 321–322. Also see Kuitenbrouwer "Privacy" 7–10; Sentrop*Privacy-bescherming* 41–62; De Graaf *Privacy en persoonsgegevens* 1–7; Overkleeft-Verburg *De Wet Persoonsregistraties* 35–59 (for a summary in English, see 699–700).

37 See De Graaf *Privacy en persoonsgegevens* 1; Nugter *Transborder flow of personal data* 145.

38 Kuitenbrouwer et al *Drieluik privacybescherming* 5.

would be divided in two and that the part with the personal information would be kept separate from the statistical information, it was nevertheless feared that the two parts could be brought together through the use of the unique number that was on every card. Memories of the Second World War when the meticulously kept record system of information on Dutch citizens was put to use by the Nazi invaders undoubtedly played a part in the protest that followed.[39]

At the same time, another contentious issue was the plan by the government to modernise the municipal register office by setting up an automated central population registry and introducing general personal identification numbers.[40]

These objections culminated in widespread civil protests against the 1971 census.[41] Organisations like Comite Waakzaamheid and Amnesty International also took part in the debate in opposition to the census.[42] So large was the number of people who refused to cooperate that the census was deemed a failure, and no census was ever attempted again.[43]

Consequently, in 1972 the government appointed a commission under the chairmanship of Koopmans (the Koopmans Commission).[44] The commission's terms of reference were to advise on the desirability of the regulation of privacy in respect of the use of automated registration systems for personal data files. The Koopmans Commission published an interim report two years later, and a final report in

39 Kuitenbrouwer et al *Drieluik privacybescherming* 6. Also see Overkleeft-Verburg *De Wet Persoonsregistraties* 41–42. Also see ch 1 par 1.1.

40 Kuitenbrouwer et al *Drieluik privacybescherming* 8–14.

41 According to Kuitenbrouwer et al *Drieluik privacybescherming* 4 the Netherlands lost its "informational innocence" (*informationele onschuld*) on 28 Febraury 1971 (the date on which the census started). Also see De Graaf "Wet Persoonsregistraties" 362.

42 Kuitenbrouwer et al *Drieluik privacybescherming* 6.

43 Overkleeft-Verburg *De Wet Persoonsregistraties* 699. She points out (46) that the failure of the 1971 census, resulting in the abolition of the use of *volkstelling* (census) as a means of gathering information by the government, was not necessarily a privacy gain, since alternative means of gathering information had to be found, which could result in more serious privacy invasion.

44 *Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties* KB 21 February 1972 nr 70 (quoted in Nugter *Transborder flow of personal data* 145 fn 1).

1976.[45] The final report was accompanied by a draft Bill.

Three themes emerged from the Koopmans report and draft Bill:[46]

- There is a necessity for transparency when personal information is collected and used.
- The data subject should have rights, especially the right to have access to the information and the right to correct any inaccuracies in the information.
- There should be supervision by the government.

It was not until 1981 that the government produced its own Bill on Personal Data Files (Wetsontwerp op de Persoonsregistraties (WPR Bill)); this Bill was based largely on the principles suggested by the Koopmans report. However, the Bill was severely criticised for its length and complexity, its division of personal data files into three categories, each with its own regime, and its emphasis on self-regulation.[47]

In November 1982 a new government took office. It appointed a new Commission, the Van der Grinten Commission, to look at the WPR Bill. The Van der Grinten Commission stated that legislation on the protection of individual privacy was necessary for three reasons:[48]

- to implement the 1983 amendment to the Constitution (since article 10(2) and 10(3) required the creation of such legislation within five years, that is in 1988)[49]
- to give effect to the Government's wish to ratify the Council of Europe Convention[50]
- to benefit the Dutch information technology industry (because legislation in other European

45 *Privacy en Persoonsregistratie: eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties* 1976 (qouted in Nugter *Transborder flow of personal data* 145 fn 2.)

46 See Berkvens & Prins "Van WPR naar WBP" 321.

47 See Nugter *Transborder flow of personal data* 146; De Graaf "Wet Persoonsregistraties" 364.

48 See Nugter *Transborder flow of personal data* 146.

49 See par 3.

50 A country may only ratify the Convention if it has data protection legislation in place (see chap 3 par 3).

countries made it possible to prohibit the transfer of personal data to countries without such legislation)

Another recommendation of the Commission was that the Bill should be simplified. The Bill was withdrawn in 1984, and a new draft Wet Persoonregistraties was published in 1985. It differed from the previous Bill in that the substantive norms relating to the protection of privacy were included in the new Bill. The emphasis on self-regulation remained.[51]

The adoption of legislation became a necessity as the deadline imposed by the Constitution for legislation in this area loomed.[52] The legislator also wanted to introduce a social security number (*sociaal-fiscaal nummer*) in order to prevent fraud.[53] This was politically acceptable only if there was legislation in place to protect privacy in personal information.[54]

After the government had initially failed to refute criticism by the First Chamber of the Dutch legislature, the Wet Persoonsregistraties was finally passed in December 1988 and officially published on 6 January 1989. It came into operation on 1 July 1989.[55]

With the adoption of the WPR, ratification of the European Convention on data protection became possible, provided specific rules governing the treatment of sensitive information were also adopted. This was done in 1993 with the Besluit Gevoelige Gegevens[56] (Decision on Sensitive Information) and on 23 August 1993 the Convention came into operation in the Netherlands.[57]

51 See De Graaf "Wet Persoonsregistraties" 365; Nugter *Transborder flow of personal data* 147.

52 See Nugter *Transborder flow of personal data* 147.

53 See Kuitenbrouwer et al *Drieluik privacybescherming* 13.

54 See Berkvens & Prins "Van WPR naar WBP" 322.

55 *Stb* 1988 655.

56 *Stb* 1993 158.

57 *Stb* 1993 158, qouted in Berkvens & Prins "Van WPR naar WBP" 322 fn 16. The Netherlands is also a (continued...)

4.2.2 European Union Directive on data protection and WBP

Initially it was thought that adoption of the European Convention on data protection by all the member countries of the European Community would be sufficient to establish a uniform level of protection of privacy in personal information. A uniform level of protection was necessary in a single market as envisaged by the European Community Treaty, otherwise one country could prevent the export of personal information to another country which did not offer sufficient protection of privacy in personal information.

However, ratification of the Convention by the European Community member states was slow,[58] and the European Commission became concerned over discrepancies in the member states' laws. In the end, the European Commission and Parliament adopted a Directive on data protection on 24 October 1995.[59] Member states were given three years in which to implement the Directive,[60] in other words, by 24 October 1998 member states were expected to have adopted legislation that complied with the provisions of the Directive.

In the Netherlands, the WPR therefore had to be amended to ensure that its principles complied with the Directive.[61] At the same time, recommendations to improve the WPR[62] were also implemented.[63] The end result was the Wet Bescherming Persoonsgegevens (WBP) (Personal Data Protection Act)

57(...continued)
member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines (see ch 3 par 2).

58 See ch 3 par 4.1.

59 Dir 95/46/EC. See ch 3 par 4.

60 Dir 95/46/EC a 32.

61 See Schreuders 1998 (2) *Priv & Inf* 52. For a comparison of the WPR with the Directive, see Berkvens & Prins "Van WPR naar WBP" 315–368.

62 See, eg, the juridical evaluation by Overkleeft-Verburg*De Wet persoonsregistraties* and the social-scientific (*sociaal-wetenskappelijke*) evaluation by Prins et al *In het licht van de Wet Persoonsregistraties*.

63 For a comparison of the WPR with the WBP, see Holvast 1998 (1) *Priv & Inf* 4.

of 2000.[64] The Act was not implemented by the 24 October 1998 deadline,[65] but came into force in September 2001.[66]

4.3 Provisions of WBP[67]

4.3.1 Overview of structure of WBP

The WBP is divided into 12 chapters, dealing with the following:

- ❒ General provisions (definitions and scope of the Act – articles 1–5)
- ❒ Conditions for the lawful processing of personal data
  - Section 1: Processing of personal data in general (articles 6–15)
  - Section 2: Processing of special personal data (articles 16–24)
- ❒ Codes of conduct (articles 25–26)
- ❒ Notification and prior investigation
  - Section 1: Notification (articles 27–30)
  - Section 2: Prior investigation (articles 31–32)
- ❒ Information provided to the data subject (articles 33–34)
- ❒ Rights of the data subject (articles 35–42)
- ❒ Exceptions and restrictions (articles 43–44)
- ❒ Legal protection (articles 45–50)
- ❒ Supervision
  - Section 1: The Data Protection Commissioner (articles 51–61)
  - Section 2: The data protection officer (articles 62–64)
- ❒ Sanctions (articles 65–75)

64 *Stb* 2000 302. The Act was passed by the Upper House of the Dutch Parliament on 3 July 2000.

65 On the consequences of this failure for the Netherlands, see Blas 1999 (1) *Priv & Inf* 8.

66 See Hustinx "The case of data protection" 285; EPIC *Privacy and human rights* 272.

67 For a brief discussion on the WBP in Dutch, see Nouwt 1998 (3) *Priv & Inf* 100, 101.

Section 1: Administrative fines (articles 66–74)

Section 2: Penal sanctions (article 75)

- ❒ Transfer of data to countries outside the European Union (articles 76–78)
- ❒ Transitional and final provisions (articles 79–83)

4.3.2 Purpose of WBP

The purpose of the first general data protection legislation (the WPR) was threefold: to secure protection for individual privacy by implementing articles 10(2) and 10(3) of the Constitution;[68] to enable the Dutch government to ratify the Council of Europe Convention;[69] and to protect the Dutch information technology industry.[70] These purposes also hold good for the new data protection legislation (the WBP), but one purpose has been added, namely to bring the Dutch data protection legislation in line with the requirements of the data protection Directive.[71]

4.3.3 Scope of WBP

Three aspects are relevant here: the scope of the WBP as determined by its definitional framework, specific exclusions from the scope of the WBP laid down in the WBP itself, and the scope of the WBP as it relates to territorial application.

4.3.3.1 Definitional framework

The WBP applies to the **full or partly automated processing** of personal data, and the **non-automated processing** of personal data which have been entered in a file or where there is an intention

68 See par 3.

69 See par 4.2.1.

70 See par 4.2.1.

71 WBP *Memorie van toelichting* (explanatory memorandum) 5.

of entering such data in a file.[72] This is a departure from the WPR which did refer to processing but focused on the existence of a personal data file.[73] The emphasis in the WBP on the other hand is on the processing of personal data (*verwerking van persoonsgegevens*). It is evident that this shift was necessary in view of the provisions of the Directive,[74] and it reflects the change that took place from the WPR to the WBP, from having a registered data file as the object of protection to having the processing of personal data, irrespective of whether they are in a file or not, as the object of protection.[75]

It is important to note that no distinction is made between the processing of data in the **private** and the **public sectors**, and the WBP applies equally to both areas.[76]

a Personal data

Personal data (*persoonsgegevens)* are defined as information (*gegeven*) relating to an identified or identifiable natural person,[77] known as the **data subject** (*betrokkene)*.[78] From this definition it is evident that to qualify as personal data, the information must concern a "natural" person. **Natural persons** by definition exclude juristic persons, and it is therefore apparent that the **WBP does not apply to juristic persons**.[79] A less obvious issue is whether dead persons are considered to be

72 WBP a 2(1) – "Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen".

73 Nugter *Transborder flow of personal data* 151.

74 WBP *Memorie van toelichting* 16.

75 Also see Holvast 1998 (1) *Priv & Inf* 4, 5.

76 Holvast 1998 (1) *Priv & Inf* 4, 6; Hustinx "The case of data protection" 285.

77 WBP a 1(a) – "persoonsgegeven: elk gegeven betreffende een geïdentificeerde of entificeerbare natuurlijke persoon".

78 WBP a 1(f) – "betrokkene: degene op wie een persoonsgegeven betrekking heeft".

79 This is also the case in the Directive (see Dir 95/46/EC a 2(a)).

"natural" persons. Dutch commentators argue that they are not.[80] Information concerning dead persons is therefore probably not considered personal data in terms of the WBP, unless such information also contains data concerning living persons.[81]

Two other issues arise from the definition of "personal data" that influence the scope of application of the WBP: First, in order to qualify as personal data the data item must "relate to" a natural person, and second, the person must be "identified" or at least be "identifiable". Under the WPR, it was required that there should be a legally relevant connection between the person and the data for the latter to qualify as personal data.[82] However, the Directive no longer appears to permit such a restricted interpretation.[83] As regards the second issue, namely the ability to identify the individual, it is argued[84] that a person is identifiable if that person's identity can be established from the data without a disproportionate amount of effort.[85]

80 See Berkvens & Prins "Van WPR naar WBP" 326. English commentators seem to have a different approach (see Pounder & Kosten 1995 issue 21 *Data Protection News* 6 and ch 3 par 4.2.3).

81 Berkvens & Prins "Van WPR naar WBP" 326

82 Nugter *Transborder flow of personal data* 151–15; Berkvens & Prins "Van WPR naar WBP" 326.

83 WBP *Memorie van toelichting* 46. See Berkvens 1995 *Computer L & Prac* 38–44 for criticism of the broad definition of "personal data" in the Directive.

84 In the explanatory memorandum accompanying the WBP (see WBP *Memorie van toelichting* 47).

85 Effort may take the form of either time, money or human resources (see Nugter *Transborder flow of personal data* 152). Two factors that play a role in this regard are identified, namely the nature of the data, and the possibility that the responsible party (for a definition of the responsible party, see text to fn 93) can accomplish the identification. As regards the nature of the data, the explanatory memorandum differentiates between directly and indirectly identifiable data. Directly identifiable data might be a name, address and date of birth, which could lead directly to the identification of a person. Because these data are unique to a person they are also used on a daily basis in commerce to distinguish between persons. Indirectly identifiable data are data that could not directly lead to the identification of a person, but could in combination with other data be connected to a specific person. An example of this would be biometric data, such as a voice print or a fingerprint which are unique to a person and which, in combination with other data, could lead to the identification of a person (see WBP *Memorie van toelichting* 48). The context in which data are used can play a role in determining the identification of a person. Singleton 1995 *Computer L & Prac* 140 gives the following example that illustrates this point. Companies holding data which indicate eg which proportion of a work force is black, Roman Catholic or homosexual would not be holding personal data as such data would not make it possible for a person to be identified. However, if there were only one black person on the list of employees then the data would enable the person to be "identified" and the data would then become personal data.

As far as the possibility of accomplishing the identification is concerned, regard should be had

(continued...)

The Directive also applies to **sound** and **image data**. The Commission of the European Union is required to examine the application of the Directive to the processing of sound and image data relating to natural persons and submit appropriate proposals.[86] While awaiting these proposals, the Dutch government has not inserted any specific provision on the processing of sound and video data into the WBP.[87] However, even under the old WPR it was assumed that photographic material falls within the scope of data protection legislation.[88]

b Processing of personal data

Processing of personal data (*verwerking van persoonsgegevens*) is defined as any operation or any set of operations concerning personal data, including the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking together as well as blocking, erasure or destruction of data.[89] The collection (*verzameling*) of personal data is further defined as the

85(...continued)
to all possible means that could reasonably be expected to be used by a responsible party or the party receiving the data, to identify the person. The current level of technology should also be taken into consideration, because with the advancement in technology it may become possible to identify a person from data where previously it would have taken a disproportionate amount of effort (WBP *Memorie van toelichting* 49).

86 Dir 95/46/EC a 33. Also see Nouwt 1998 (3) *Priv & Inf* 100, 101.

87 WBP *Memorie van toelichting* 70.

88 Berkvens & Prins "Van WPR naar WBP" 326. Loose photographs kept at random in a box, or in a photo album, do not fall within the provisions of the WBP, since they are not processed automatically, nor do they form part of a structured set of data as required by a 2(1). However, digitally processed photos or sound recordings which can be automatically processed, undoubtedly do fall within the scope of the Act (see WBP *Memorie van toelichting* 70).

89 WBP a 1(b) – "verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens". The WPR did not define "processing". This is therefore a new definition in the WBP, and it follows the definition given in the Directive (Dir 95/46/EC a 2(b)).

obtaining of personal data.[90] The inclusion of the collection of data in the definition of processing goes further than the WPR,[91] and implies that provisions of the WBP are already applicable at this early stage.[92]

c Responsible party and processor

The **responsible party** (*verantwoordelijke*) is the natural person who, or legal person or administrative body which, alone or in conjunction with others, decides on the purpose and means of processing personal data.[93] The responsible party is a new concept which has been introduced into the WBP because of the provisions of the Directive, and replaces the term "holder" (*houder*) used in the WPR. The term "responsible party" should be interpreted as referring to the person who in the legal-technical (*formeel-juridisch*) (as opposed to factual) sense has the authority to determine the purposes of the processing.[94] The **processor** (*bewerker*) is the person who processes personal data for the responsible party, without being subject to the direct authority of that party.[95] In other words, the processor would be outside the hierarchy of the responsible party, and have no say over the use of the data or the distribution of the data to third parties.[96]

---

90 WBP a 1(o) – "verzamelen van persoonsgegevens: het verkrijgen van persoonsgegevens".

91 WBP *Memorie van toelichting* 50.

92 Eg, the purpose for which the data are going to be processed must be determined before the data are collected (WBP *Memorie van toelichting* 51. Also see Holvast 1998 (1) *Priv & Inf* 4, 5). Some commentators feel that the definition of processing is too wide, and will unnecessary include supplementary activities that are not true processing activities, such as making temporary back-up files, or the activities of service providers who merely transport data with no knowledge of their content (see Berkvens & Prins "Van WPR naar WBP" 327).

93 WBP a 1(d) – "verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt". The Directive uses the term "controller" (Dir 95/46/EC a 2(d)).

94 WBP *Memorie van toelichting* 55.

95 WBP a 1(e) – "bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen".

96 WBP *Memorie van toelichting* 61–62.

d File

In the case of **non-automated processing**, the personal data must be entered in a file (*bestand*) or there must be an intention of entering the data in a file.[97] A file is defined as any structured set of personal data, regardless of whether or not this data set is centralised or dispersed along functional or geographical lines that is accessible according to specific criteria and relates to different persons.[98] This definition follows the definition of a "filing system" given in the Directive,[99] except for the last part, namely that it must relate to different persons.[100] The WBP shares this provision with the WPR. This means that a file containing data relating to one person only is not a personal data file within the meaning of the WBP.[101]

Another important provision is that the personal data should be a "structured set" (*gestructureerde geheel*) of personal data. The term *geheel* implies that the data should have something in common that binds them together.[102] This could, for example, be a common destination, or the fact that they are in practice considered to belong together. It is also important to note that the purpose for which they are processed should be similar.[103]

Lastly, in order to be a file within the terms of the WBP, the data must be accessible according to specific criteria. What is required is *systematische toeganklijkheid*, in other words there should be

97 WBP a 2(1).

98 WBP a 1(c) – "bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen".

99 Dir 95/46/EC a 2(c).

100 The explanatory memorandum to the WBP points out that the Directive allows member states "een zekere marge voor de invulling van dit begrip" (WBP *Memorie van toelichting* 53).

101 Nugter *Transborder flow of personal data* 151.

102 "Het vereiste 'gestructureerde geheel' ... houdt in dat de gegevenswerking ... op grond van meer dan één kenmerk onderlinge samehang moet(-en) vertonen." See WBP *Memorie van toelichting* 54.

103 Back-up files should, eg, not be considered to be a filing system separate from the original filing system (WBP *Memorie van toelichting* 54).

a structure to the data that makes them accessible in a systematic way.[104] Simple dossiers that are merely alphabetically and lexicographically accessible will in most instances not satisfy this requirement.[105]

e Data subject, third party and recipient

The **data subject** (*betrokkene*) is the person to whom the personal data relates.[106] In the WPR the data subject was called the *geregistreerde*.[107] The new term again reflects the shift in emphasis from the WPR to the WBP. In the WPR a registered data file was the object of protection whereas in the WBP the data subject's personal data are themselves the object of protection.

Other parties, apart from the data subject, the responsible party and the processor, who may be involved in the processing of personal data are the third party and the recipient. The **third party** is any party other than the data subject, the responsible party, the processor, or any person coming under the direct authority of the responsible party or the processor who is authorised to process personal data.[108] The **recipient** is any person to whom data are supplied.[109] The recipient may be a third party, or a person within the organisation of the responsible party.[110]

4.3.3.2 Exclusions from scope

104 WBP *Memorie van toelichting* 54.

105 Nugter *Transborder flow of personal data* 151.

106 WBP a 1(f). For the wording of this section, see fn 78 above.

107 Since both terms (*betrokkene* and *geregistreerde*) are translated as "data subject", the difference between the two terms is not reflected in English.

108 WBP a 1(g) – "derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken".

109 WBP a 1(h) – "ontvanger: degene aan wie de persoonsgegevens worden verstrekt".

110 The importance of the term "recipient" (*ontvanger*) lies in the duty of the responsible party to give information about recipients in certain circumstances (see text to fn 281, 292, 333).

As allowed by the Directive,[111] the WBP specifically excludes from its scope the processing of personal data in the course of any purely **personal or household activity**.[112] A personal activity would, for example, refer to the keeping of a list of names and addresses by a person on individuals with whom that person has regular contact, as long as the list is not used by other persons as well.[113] A household activity refers to the use of personal data within a family. In this case more than one person may use the personal data, as long as they belong to a well-defined group of persons (namely the family).[114]

Also excluded are processing activities that fall under **other legislation**, namely the Wet op de Inlichtingen en -Veiligheidsdiensten (Intelligence and Security Services Act),[115] the Wet op Politieregisters (Police Files Act),[116] the Wet Gemeentelijke Basisadministratie Persoonsgegevens (Municipal Database (Personal Records) Act),[117] the Wet op de Justitiele Documentatie en op de Verklaringen

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

112 WBP a 2(2)(a).

113 WBP *Memorie van toelichting* 70. Also see Nouwt 1998 (3) *Priv & Inf* 100, 101.

114 WBP *Memorie van toelichting* 70.

115 *Stb* 1987 635. See WBP a 2(2)(b).

116 *Stb* 1990 414. WBP a 2(2)(c) refers to processing of personal data for the purposes of implementing the police tasks defined in a 2 of the Police Act 1993. Although the definition of police tasks is to be found in the Police Act, the Police Files Act is the data protection legislation for police files. The Dutch legislator has decided on a separate law for police files, because the data processed by the police are very sensitive and usually not furnished voluntarily, or not supplied by the data subject, or sometimes the data subject is not even aware that the police have the information. As Dr Ulco van de Pol (Vice-President of the Dutch data protection authority) put it in an address in 1995 in Copenhagen: "In short, information which justifies laying down the strictest and hence most specific possible requirements for their collection, storage and use." The aim of the Police Files Act is to create a "closed system of supplying data" (*geslote verstrekkingsregime*). Within the police organisation there is a free flow of information as regards the police function. Data may only be supplied outside this closed system in cases specifically prescribed or allowed by the Act, eg to judicial and governmental authorities, organisations for the assistance of victims and insurance companies for handling claims.

117 *Stb* 1994 494. See WBP a 2(2)(d). The Wet Gemeentelijke Basisadministratie Persoonsgegevens has taken the place of the population register since 1994. It is a fully automated information system containing the population information of each municipality (*gemeente*). The information is used to complete municipal tasks, and to provide services, such as the issuing of driver's licences or passports. Information in this information system is also given to other government institutions such as the police, the justice department and the tax service. Information may only be supplied to other institutions in a limited manner and only on

(continued...)

omtrent het Gedrag (Judicial Records and Certificates of Good Behaviour Act),[118] and the Kieswet (Electoral Provisions Act).[119] Processing by the **armed forces** is also excluded 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 (College Bescherming Persoonsgegevens, hereafter referred to as the CBP),[120] of such a decision as quickly as possible.[121]

Further, the WBP is not applicable in its totality to the processing of personal data for exclusively **journalistic, artistic or literary purposes**. Under the WPR, personal data files held exclusively for journalistic purposes by the press, radio or television were totally exempted from the scope of the Act.[122] However, owing to the provisions of the Directive on data protection, this is no longer permissible. The Directive requires member states to provide for certain exemptions or derogations[123] in their data protection legislation where personal data are processed solely for journalistic purposes or for the purposes of artistic or literary expression, if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[124] From this, it is evident that the processing

117(...continued)
the basis of a municipal ordinance (*Persberichten*: *Beveiliging bevolkingsgegevens onvoldoende Registratiekamer onderzocht bevolkingsadministratie gemeenten* (18 February 1999) on the website of the Dutch data protection authority (the College Bescherming Persoonsgegevens, formerly the Registratiekamer (http://www.cbpweb.nl/). Also see Mutsaers 1998 (3) *Priv & Inf* 109).

118 *Stb* 1955 395. See WBP a 2(2)(e).

119 *Stb* 1989 423. See WBP a 2(2)(f).

120 Formerly known as the Registratiekamer. See par 4.3.11.1 on the powers and functions of the CBP.

121 WBP a 2(3). This refers to the processing of personal data by military personnel during an actual military operation outside the Netherlands, eg during international crisis management situations (see WBP *Memorie van toelichting* 72).

122 WPR a 2.

123 Specifically from the provisions relating to the lawfulness of processing, the rules relating to the transfer of data to third countries, and the provisions relating to the supervisory authority and the working party established by the Directive.

124 Dir 95/46/EC a 9. This provision is necessary in order for the Directive to give effect to s 10 of the European Convention on Human Rights, which declares that "everyone has the right to freedom of expression" and (continued...)

of personal data for journalistic, literary and artistic purposes must in principle also fall under the provisions of the Act implementing the Directive.[125] The WBP consequently excludes some, but not all, of the provisions of the Act when personal data are processed for journalistic purposes or for the purposes of artistic or literary expression.[126]

The following provisions remain applicable when personal data are processed for exclusively journalistic, artistic and literary objectives: the provisions of chapter 1 (definitions, scope and jurisdiction); articles 6 to 11 and 13 to15 (dealing with the general rules on the lawfulness of processing, except article 12); article 25 (providing that codes of conduct may be adopted by organisations) and article 49 (giving the data subject a right to fair compensation for non-patrimonial damage because the provisions of the WBP were not complied with).[127]

4.3.3.3 Territorial application / applicable national law

The WBP applies to the processing of personal data in connection with the activities of an establishment

124(...continued)
that this right includes the right "to receive and impart information". The member states may, however, not lay down exemptions from the security principle (see par 4.3.4.1). The supervisory authority should also have *ex post* powers, eg to publish a regular report or to refer matters to judicial authority (see Dir 95/46/EC recitals par (37)). The provisions of a 9 naturally also apply to the processing of sound and image data carried out for journalistic purposes, or for the purposes of literary or artistic expression (Dir 95/46/EC recitals par (17)).

125 WBP *Memorie van toelichting* 73.

126 WBP a 3(1).

127 Ie, the WBP exempts personal data being processed for journalistic, artistic and literary purposes from the following provisions: a 12 (prohibiting any processing of data by anyone who has access to the data, including the processor, unless instructed to do so by the responsible party or required to do so by law, and placing a duty of confidentiality on the processor); a 16 (prohibiting the processing of sensitive data), a 17–24 (exemptions from a 16, which become redundant once a 16 is not applicable); a 26 (providing that more detailed rules may be applied by general administrative order to a particular sector concerning the general rules on lawfulness of processing); chapter 4 (ie a 27–32, dealing with the prior investigation of processing activities); chapter 5 (a 33 and 34, dealing with the information that must be provided to the data subject); chapter 6 (a 35–42, dealing with the rights of the data subject); chapter 7 (a 43–44, dealing with exceptions and restrictions); chapter 8 (a 45–48, and 50, dealing with legal protection). As already indicated, a 49 (right to compensation for patrimonial and non-patrimonial damages) remains applicable.

of a responsible party in the Netherlands.[128] It also applies to the processing of personal data by or for responsible parties who are not established in the European Union, but use automated or non-automated means situated in the Netherlands (unless these means are used only for forwarding personal data).[129] In the latter case, the data processing may only take place if the responsible parties have designated a person or body in the Netherlands to act on their behalf in accordance with the provisions of the WBP. For the purposes of the WBP such a person or body must be deemed to be the responsible party.[130] Noncompliance with this provision is punishable by a fine or, if it was deliberate, by a prison sentence not exceeding six months.[131]

Because of the fact that data are gaining a more and more immaterial character, jurisdiction can no longer be based on the place where the data are being kept. Instead, the place where the responsible party is situated becomes the basis for jurisdiction. But if the responsible party is situated outside the European Union a concession is made and the place where the data are processed becomes relevant.[132] This also means that if data are processed inside the Netherlands on behalf of a responsible party situated in another European Union member country, the Dutch courts have to apply the law of the foreign country, which may differ from Dutch law, as long as it remains within the parameters allowed by the Directive.[133]

4.3.4 Conditions for the lawful processing of personal data

128 WBP a 4(1).

129 WBP a 4(2). The Directive also provides for one other situation where the national law of the particular member state will apply, namely where the responsible party is established in a place where its national law applies because of international public law (Dir 95/46/EC a 4(1)(b)). The Dutch legislator did not include a similar provision, because it was considered unnecessary to do this. In terms of public international law, Dutch law, including the WBP, automatically applies to Dutch ships, aeroplanes and embassies (WBP *Memorie van toelichting* 77).

130 WBP a 4(3).

131 See WBP a 75 and WBP *Memorie van toelichting* 77.

132 WBP *Memorie van toelichting* 75.

133 WBP *Memorie van toelichting* 75–76.

The Directive lays down general rules determining under what circumstances personal data may lawfully be processed. It is up to the member states to determine more precisely what specific conditions should be adhered to.[134] The WBP distinguishes between the processing of personal data in general[135] and the processing of special (that is sensitive) personal data.[136]

4.3.4.1 Processing of personal data in general

The responsibility is imposed on the responsible party[137] to ensure that personal data are processed in accordance with the law and in a proper and careful manner (*behoorlijke en zorguldige wijze*).[138] The Directive uses the terms "fairly and lawfully".[139] The Dutch government chose not to follow this wording, because it considered it to be tautological: if processing is unfair it is also unlawful. Saying that the processing must be in accordance with the law amounts to stating that the data must be processed lawfully. It was felt that the requirement that processing must be done "behoorlijk en zorguldig" is a better reflection of the standard required in society to prevent an unlawful act.[140]

The WBP spells out specific principles that must be complied with to ensure that processing is lawful. These principles, all based on the requirements of the Directive, will be dealt with next.

a Purposes for which data are collected

134 Dir 95/46/EC a 5.

135 WBP ch 2 s 1.

136 WBP ch 2 s 2.

137 WBP a 15.

138 WBP a 6. Schreuders describes a 6 as *het moederartikel* in the WBP when dealing with personal data, and indicates that it is the legality principle for the processing of data. He points out that the articles following on a 6, namely a 7, 8 and 9, describe what can or cannot be considered "proper and fair" (Schreuders 1998 (2) *Priv & Inf* 52, 53–54).

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

140 WBP *Memorie van toelichting* 78.

First of all, the collection of personal data must be for specific, explicitly defined and legitimate purposes (*doeleinden*).[141] These purposes must be established before any data are collected, and may not be vague, uncertain or illegitimate. 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, further processing that may be done, etcetera. The Dutch commentators refer to this principle as *doelbinding*.[142]

b Grounds for legitimate processing

Following the Directive,[143] the WBP spells out the only six conditions[144] under which personal data may lawfully be processed:[145]

i Data subject has unambiguously consented[146]

Consent of the data subject is defined[147] as any freely given, specific and informed expression of will

141 WBP a 7.

142 Ie, binding by purpose or objective. See WBP *Memorie van toelichting* 78; Schreuders 1998 (2) *Priv & Inf* 52, 55.

143 Dir 95/46/EC a 7.

144 It is crucial that every processing of personal data must be based on one or more of these grounds (Schreuders 1998 (2) *Priv & Inf* 52, 54).

145 Note, however, that a duty of confidentiality cannot be set aside because one of the grounds for processing is present (see WBP a 9(4) and see text to fn 174). Also see WBP *Memorie van toelichting* 94. Furthermore, the constitutional principles of proportionality and subsidiarity should also be taken into account in every instance where data are processed (WBP *Memorie van toelichting* 80). Proportionality means that the infringement of privacy of the data subjects should not be out of proportion to the purpose that is served, and in terms of the subsidiarity principle processing should not be done if the purpose for which the processing is done could be accomplished in a less intrusive manner. On these principles, see WBP *Memorie van toelichting* 8–9.

146 WBP a 8(a).

147 WBP a 1(i) – "toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt".

whereby data subjects agree to the processing of personal data relating to them.[148] In this regard, three issues are important:[149] First, the data subjects should have been able to freely express their will, and should actually have done so. There is no legal consent if data subjects were forced to consent as a result of circumstances or pressured to do so by a particular relationship in which they stand.

Second, the expression of will should relate to a specific processing operation, or to a specific category of personal data. It should be evident which data will be involved, what the objectives of the processing are, and if third parties will receive the data, it should also be evident who they are going to be. A general and nonspecific authorisation to process data would not fulfil this requirement.

Third, the data subjects should have had knowledge of all the relevant information. In other words, there should be "informed consent". This implies that the processor should inform the data subjects on all aspects of the processing that may be relevant to them. This does not mean, however, that the data subjects should be informed about facts that they already have knowledge of.

The consent must furthermore be unambiguous. This implies that there should be no doubt about the fact that a data subject has consented. The onus is on the responsible party to make sure that the data subject has consented.[150] The data subject's consent (or that of the representatives where the data subject is under sixteen years of age or under curatorship)[151] may be retracted at any time.[152] The retraction of consent does not have any influence on processing that has already taken place.[153]

ii Processing is necessary for performance of a contract to which data subject is party

148 WBP a 5 is also of importance in this regard, since it provides that a person under the age of sixteen or a person under curatorship cannot consent, but the consent of such person's legal representative is required.

149 WBP *Memorie van toelichting* 65.

150 WBP *Memorie van toelichting* 66.

151 WBP a 5(1).

152 WBP a 5(2).

153 WBP *Memorie van toelichting* 67–68.

(or to complete a precontractual stage at request of the data subject)[154]

This does not refer to a contract to process data, but to a contract where the data subject is a party to the contract and the processing of data is necessary[155] for the fulfilment of the contract.[156]

iii *Processing is necessary in order to comply with a legal obligation to which responsible party is subject*[157]

The responsible party must be under a legal obligation which could only be fulfilled if the relevant personal data were processed. This would be the case for example where an employer is obliged to supply information on the income of its employees to the Receiver of Revenue.[158]

iv *Processing is necessary to protect a vital interest of data subject*[159]

Vital interest is described by the Directive[160] as an interest which is essential for the data subject's life. This clause should therefore be narrowly interpreted, and personal data should only be processed where this is a matter of life or death.[161]

---

154 WBP a 8(b).

155 The idea that the processing should be necessary for a certain purpose before it could be done lawfully is found in several articles of the WBP. The "necessity" test especially comes into play when a balancing of interests has to be done. This test is considered to be a part of the principles of proportionality and subsidiarity (see fn 145).

156 WBP *Memorie van toelichting* 80.

157 WBP a 8(c).

158 Also see WBP *Memorie van toelichting* 82–83.

159 WBP a 8(d). Initially, this ground was formulated as "combatting serious danger to the health of the data subject", but it has subsequently been amended to link up more closely with the wording of the Directive (Dir 95/46/EC a 7(d)).

160 Dir 95/46/EC recitals par (31).

161 WBP *Memorie van toelichting* 84.

v ***Processing is necessary for proper performance of a public law duty by administrative body concerned or by administrative body to which data are provided***[162]

Once again, the processing should be necessary before this ground can serve as a justification for such processing. Data subjects may at any time register objections relating to their particular circumstances with the responsible parties.[163] This is a ground on which processing in the public sector can generally be based.[164]

vi ***Processing is necessary to uphold legitimate interests of responsible party or of third party to whom data are supplied, except where interests or fundamental rights and freedoms of data subject, in particular right to protection of individual privacy, prevail***[165]

This provision is more general than the previous ones, where the processing should in each instance be tested against a specific objective or purpose mentioned in the WBP. It is a "catch all"clause (*restbepaling*) or escape valve (*uitlaatklep*) providing for those situations that do not fall within the exact terms of the other provisions, but nevertheless should be considered to be legitimate grounds for processing personal data. Both the private and the public sectors can use this provision, in contrast to the previous clause, which is only available to the public sector.[166] This provision would for example be applicable where commercial institutions need to process personal data in the performance of

162 WBP a 8(e).This provision does not use the exact wording of the Directive, because it was adapted to fit in with the General Administrative Law Act (Algemene Wet Bestuursrecht (AWB) *Stb* 315 1992) (WBP *Memorie van toelichting* 84). The General Administrative Law Act aims to codify, harmonise, systematise and simplify the Dutch administrative law. It is produced in stages: the first two stages came into force in 1994, and the third stage in 1998. A fourth stage is being prepared. For the text of the Act, see the home page of the Dutch Minister of Justice at http://www.justitie.nl.

163 WBP a 40(1). On the right to object, see par 4.3.8.3.

164 Schreuders 1998 (2) *Priv & Inf* 52, 54.

165 WBP a 8(f).

166 Schreuders 1998 (2) *Priv & Inf* 52 54.

commercial transactions.[167] This provision can only be used if the processing of the personal data is really necessary to give effect to an essential interest of the responsible party, and the processing should not unnecessarily interfere with the data subject's right to privacy. The interests of the responsible party have to be balanced against the right to privacy of the data subject.[168]

Data subjects have a right to object to processing based on the latter two grounds.[169]

c Compatible use

Another principle of the WBP is that personal data may not be processed in a way that is incompatible with the purposes for which they have been obtained.[170] In other words, personal data may be processed for another purpose than the one for which they were originally collected, provided that such purpose is compatible with the original one.[171]

167 Say eg a bank wants to make a transfer of funds from the account of the data subject to that of a third party. The data subject has consented to this transaction and a 8(a) (consent to processing) or a 8(b) (performance in terms of a contract) is applicable as far as processing of the data subject's data is concerned, but as far as the processing of personal data of the third party is concerned a 8(f) would be the applicable ground (WBP *Memorie van toelichting* 86). Processing for marketing purposes will mostly also be based on a 8(f) (see Artz, Ebbers, Schreuder & Nouwt 1998 (5) *Priv & Inf* 196 *et seq*).

168 According to Schreuders 1998 (2) *Priv & Inf* 52, 54, by including this balancing test (which he refers to as a "privacy test"), the doctrine of the horizontal application of constitutional rights is incorporated into the Act itself.

169 WBP a 40(1). Schreuders 1998 (2) *Priv & Inf* 52, 55 refers to the right to object granted by a 40 as a "relative" right to object, because it refers only to processing based on a 8(e) and 8(f). A 41 also confers the right to object, basically to processing for direct marketing. He refers to the right to object conferred by a 41 as an "absolute" right to object, because a data subject can object to processing based on any of the grounds (ie a 8(a) to 8(f)). On the right to object, see par 4.3.8.3.

170 WBP a 9(1). Also see Dir 95/46/EC a 6(1)(b). The WBP uses the double negative – ie the processing should **not** be **in**compatible with the original purpose for which it was collected. Schreuders 1998 (2) *Priv & Inf* 52, 56 argues that in legal discourse a double negative is not always interpreted to mean the same as a positive. However, the *Memorie van toelichting* uses the positive form as if it means the same as the double negative (see WBP *Memorie van toelichting* 89–94).

171 WBP *Memorie van toelichting* 90. Initially the draft WBP listed certain criteria to help the responsible parties establish whether they comply with the requirement of compatible use or not. However, these criteria were later deleted from the Act, because it was thought that they could be interpreted restrictively, whereas they were not meant to be an exclusive list (see par F *Nota van wijziging Tweede kamer vergaderjaar* 1988–1999 25 892 nr 10 December 1998). The criteria, which may in practice still prove to be relevant,

(continued...)

The WBP provides for **exemptions and restrictions** to the compatible use principle in the interests of state security; the prevention, detection and pursuit of crime; important economic and financial interests of the state and other public bodies; supervising compliance with legal provisions established in the interests of the previously mentioned two interests; and protecting the data subjects or the rights and freedoms of other persons.[172]

Processing of personal data originally collected for a different purpose, but subsequently processed for **historical, statistical or scientific purposes** will not be considered to be an incompatible use, where the responsible party has made the necessary arrangements to ensure that the further processing will only be for these specific purposes.[173]

The processing of personal data may not take place where this is precluded by an **obligation of confidentiality** established by official, professional or legal provisions.[174]

d Storage of data

The WBP also states the principle that personal data may not be kept in a form which permits identification of data subjects for any longer than is necessary for achieving the purposes for which they were

171(...continued)
are the following: the relationship between the purpose of the intended processing and the purpose for which the data have been obtained; the nature of the data concerned; the consequences of the intended processing for the data subject; the manner in which the data were obtained; the extent to which appropriate guarantees have been put in place with respect to the data subject.

172 WBP a 43. See par 4.3.9.

173 WBP a 9(2). The Directive provides that processing for historical, statistical or scientific purposes will not be considered to be incompatible, provided that the member states provide appropriate safeguards. These safeguards must in particular rule out the use of the data "in support of measures or decisions regarding any particular individual" (Dir 95/46/EC recitals par (29)). The proviso found in the WBP ("indien de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden") is the appropriate safeguard formulated by the Dutch government. In this regard the explanatory memorandum mentions that statistical data may be used for marketing purposes, as long as those purposes are not direct marketing (ie, directed at a specific person) (WBP *Memorie van toelichting* 93).

174 WBP a 9(3).

collected or subsequently processed.[175] Personal data may be kept for longer periods provided that this is for historical, statistical or scientific purposes and the responsible party has made the necessary arrangements to ensure that the data concerned are used solely for these purposes.[176]

e Data quality

The WBP provides that in principle the personal data may only be processed if they are sufficient, relevant, not excessive[177] correct and precise.[178] The sufficiency, relevance, accuracy, etcetera of the data are again determined with reference to the purposes for which they were collected or subsequently processed.[179] The responsible party must take the necessary (*nodige*) steps to ensure that the personal data are correct and accurate.[180] However, 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.[181]

f Confidentiality and security of processing

The WBP implements the principle of confidentiality and security of processing by first of all prohibiting in general any processing of data by anyone acting under the authority of the responsible party or the

175 WBP a 10(1).

176 WBP a 10(2).

177 WBP a 11(1). Ie, "toereikend, ter zake dienend en niet bovenmatig".

178 WBP a 11(2). Ie, "juist en nauwkeurig". Schreuders 1998 (2) *Priv & Inf* 52, 56 indicates that accuracy could refer to either "formal" or "material" accuracy. Formal accuracy relates to whether the information has been recorded correctly; material accuracy relates to whether the correct information has been recorded.

179 This provision will not be complied with if the processor does not have sufficient data to form the correct image of the data subject. An example will be if the processor 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. See WBP *Memorie van toelichting* 96.

180 WBP a 11(2).

181 WBP *Memorie van toelichting* 97.

processor, as well as by the processors themselves who have access to personal data, unless ordered to do so by the responsible party or required to do so by law.[182] The basic premise is that the responsible parties remain responsible and accountable for the processing,[183] but that the responsible parties can only take this responsibility if the persons under their control, or who process the data on their behalf, comply with their instructions.[184]

The WBP also requires the persons referred to above, to whom a duty of confidentiality under official, professional or legal provisions does not already apply,[185] to 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 their duties.[186]

The WBP furthermore spells out the responsibilities of the responsible party in regard to security measures. 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[187] 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.[188]

182 WBP a 12(1).

183 WBP a 15.

184 WBP *Memorie van toelichting* 97.

185 As has already been seen, the processing of personal data may not take place where this is precluded by an obligation of confidentiality established by official, professional or legal provisions (see text to fn 174). Note that WBP a 61(5) provides that no appeal is possible on the grounds of a duty of confidentiality, insofar as information or assistance is required in connection with the involvement of the CBP (data protection authority) in the processing of personal data.

186 WBP a 12(2).

187 The term "appropriate" (*passende*) indicates that the 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 (WBP *Memorie van toelichting* 99).

188 WBP a 13.

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 for the processing to be carried out. The responsible party must ensure that these measures are complied with.[189] The responsible party must also ensure that the processor complies with article 12(1)[190] and with the obligations relating to security incumbent on the responsible party.[191] Where the processor is established in another country of the European Union, the responsible party must ensure that the processor complies with the laws of that country.[192]

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.[193] In order to serve as evidence, the parts of the agreement or legal act relating to personal data protection and the security measures referred to in article 13 must be in writing or in another equivalent form.[194]

4.3.4.2 Processing of special / sensitive personal data

In compliance with the Directive,[195] the WBP prohibits the processing of personal data that concern a person's religion or philosophy of life, race, political persuasion, health and sexual life, or personal data concerning trade-union membership, except if the processing is done within prescribed limits set out in the WBP in this regard. This prohibition also applies to personal data concerning criminal records

189 WBP a 14(1).

190 Prohibiting the processing of personal data by the processor unless instructed to do so by the responsible party (see text to fn 182).

191 WBP a 14(3).

192 WBP a 14(4).

193 WBP a 14(2).

194 WBP a 14(5).

195 Dir 95/46/EC a 8.

or unlawful or objectionable conduct[196] and relating to a ban imposed with regard to such conduct.[197]

However, the Directive also allows member states to derogate from this prohibition on certain grounds.[198] Consequently, the WBP spells out general and specific grounds where the processing of sensitive personal data will not be prohibited.

a General grounds

The prohibition against the processing of sensitive personal data is in general not applicable where:[199]

- ❒ the data subject has expressly consented to the processing[200]
- ❒ the data have clearly been made public by the data subject[201]
- ❒ this is necessary to establish, exercise or defend a right in law[202]
- ❒ this is necessary to meet an obligation under international law

196 Eg, stalking someone.

197 WBP a 16 – "De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag".

198 Dir 95/46/EC a 8(2)–(5).

199 WBP a 23(1)(a)–(e).

200 On the meaning of consent, see text to fn 147.

201 The intention of the data subject to publicise the specific personal data must be manifestly evident from such person's actions. An example of this would be where a person who is running for a public office during an election publicly expresses allegiance to a specific political party. However, sensitive data may not be processed where they have been made public against the wishes of the data subject. The explanatory memorandum to the WBP gives the following interesting example: the fact that a person has a handicap may be publicly known, because it is obvious when looking at the person, but this data may not be processed in terms of this exemption, because the data have not been made known by the data subject of his or her own volition. However, should the handicapped person canvass for the interests of handicapped persons and in this manner voluntarily make known such handicap, this exemption will be applicable. See WBP *Memorie van toelichting* 123.

202 A decision of the Centrale Raad van Beroep (*CRvB* 15 Feb 1995) illustrates this exemption. In this case it was held that an employer need not pay out an amount of money to an employee who claims to be medically unfit to work if the employer had not been allowed access to the medical data of the employee (WBP *Memorie van toelichting* 124).

- this is necessary with respect to an important general interest, provided that appropriate guarantees to protect individual privacy have been given and this exemption is either provided for by law or the CBP (the data protection authority) has granted it.[203] When granting the exemption, the CBP may impose rules and restrictions. Where this type of exemption is made, the member state must notify the European Commission.[204] The notification must be made either by the relevant Minister, where the processing is provided for by law, or by the CBP, where it has granted the exemption.[205]

As seen, the Directive in many instances allows that the **processing of data for statistical or scientific purposes** be treated more leniently, because these processing activities mostly do not pose a serious threat to the privacy of individuals. The WBP also provides that the prohibition on the processing of sensitive personal data is not applicable where the processing is for scientific research or statistical purposes, provided that such research is in the general interest, that the processing of the data is necessary for the particular research or statistics, that it appears to be impossible or would involve a disproportionate effort to ask for express consent, and that sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.[206]

The prohibition on the processing of sensitive data is also not applicable if it is necessary for **journalistic, artistic or literary purposes**.[207]

The Directive does not prohibit the use of a **national identification number**, but leaves it to member

203 This is a general exemption that can be used if one of the other exemptions does not specifically fit the situation (WBP *Memorie van toelichting* 124).

204 Dir 95/46/EC a 8(6).

205 WBP a 23(3).

206 WBP a 23(2).

207 WBP a 3(2). Also see par 4.3.3.2 above.

states to determine the conditions under which such a number may be processed.[208] The WBP provides that when a law prescribes that a number will be associated with a person in order to identify that person, then 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 the Act.[209]

Cases other than those referred to above may be designated by general administrative regulation in which a number to be indicated in this connection can be used. More detailed rules may be laid down concerning the use of such a number.[210]

b Specific grounds

The specific grounds where processing of sensitive personal data is allowed depend on the type of sensitive data involved:

i Personal data relating to religious or philosophical beliefs

The Dutch Constitution guarantees freedom of religion or philosophy of life.[211] Consequently, the WBP has to make concessions to churches and other institutions involved in providing religious care in cases where they process the personal data of their members or persons in their care.[212]

Church associations or other associations founded on spiritual principles may process the personal data

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

209 WBP a 24(1). Ie, where legislation introduces a specific number, such as the so-called *sofi-nummer* (*sociaal-fiscaal* or social-fiscal number) or the *A-nummer* (administration number) introduced by the Wet Gemeentelijke Basisadministratie (Municipal Database (Personal Records) Act) (*Stb* 1994 494), then the number may be used only for purposes that conform to the purpose of the legislation introducing the number. See WBP *Memorie van toelichting* 127–128.

210 WBP a 24(2).

211 Dutch Constitution a 6.

212 WBP *Memorie van toelichting* 103.

of their members,[213] as well as of any member's family members, provided that the association maintains regular contact with these family members in connection with the purpose for which it was established and the family members have not objected thereto in writing.[214] Institutions founded on religious or philosophical principles may also process data provided that this is necessary for the aims of the institutions and the achievement of their principles.[215] Other institutions that provide spiritual care[216] may process sensitive personal data in so far as this is necessary for the spiritual welfare of the data subjects, unless they have objected in writing to the processing.[217] In all of the above instances, the data may not be disclosed to a third party without the consent of the data subject.[218]

ii Personal data relating to race

The prohibition on the processing of data that reveal someone's race (*ras*)[219] is not applicable in two instances: First of all, if the purpose of the processing is to identify data subjects and it is essential to refer to race.[220] Secondly, if the purpose is to assign a preferential status to persons belonging to a specific ethnic or cultural minority group, with a view to reducing or eradicating actual inequalities that exist. The following conditions must be met in such a case:

213 WBP a 17(1)(a).

214 WBP a 17(2)(a) and (b).

215 WBP a 17(1)(b).

216 Eg, the spiritual care that takes place in the army, retirement homes or hospitals (WBP *Memorie van toelichting* 124).

217 WBP a 17(1)(c).

218 WBP a 17(3).

219 In the Directive (Dir 95/46/EC a 8) the terms "racial and ethnic origin" are used, but in Dutch law the concept of "race" is understood to include "ethnic origin", and therefore only the term "race" is used (WBP *Memorie van toelichting* 102). The term "race" should therefore be interpreted widely, and include skin colour, origin, and national or ethnic descent (see WBP *Memorie van toelichting* 104).

220 WBP a 18(a). Where employers take pictures of their employees, eg in order to issue them with security cards, and then store these pictures in a data bank where they can be automatically accessed, processing of personal data is taking place. Such pictures may reveal the race of a person. The above-mentioned exemption is intended to cover such situations (WBP *Memorie van toelichting* 105).

- ❒ It must be necessary to process the data for that purpose.

- ❒ The data must relate only to the country of birth of the data subjects, their parents or grandparents, or relate to other criteria, determined by law, by means of which it can objectively be determined that a person belongs to a minority group.
- ❒ The data subjects have not objected in writing to the processing.[221]

iii Personal data relating to political persuasion

Personal data revealing a person's political persuasion (*politieke gezindheid*) may be processed in two instances: Firstly, by institutions founded on political principles[222] with respect to their members or employees or other persons belonging to the institution, provided that the processing is necessary for the aims of the institution and the achievement of its principles.[223] The personal data may not be disclosed to a third party without the consent of the data subject.[224] Secondly, "met het oog op de eisen die met betrekking tot politieke gezindheid in redelijkheid kunnen worden gesteld in verband met de vervulling van functies in bestuursorganen en adviescolleges" (with a view to the requirements concerning political persuasion which can reasonably be applied in connection with the performance of duties in administrative and advisory bodies).[225]

iv Personal data relating to trade union membership

221 WBP a 18(b). There may be instances where racial data may incidentally be recorded, eg where a school, in order to identify the pupils, records the place of birth of all the pupils. In such a case the processing of personal data may indirectly relate to sensitive personal data – ie, the processing may perhaps reveal the racial origin of a pupil. However, the purpose of the processing would not be to record racial origin, and it is therefore argued that this type of processing activity falls outside the prohibition on the processing of sensitive data (WBP *Memorie van toelichting* 106).

222 Eg a political party.

223 WBP a 19(1)(a).

224 WBP a 19(2).

225 WBP a 19(1)(b). I interpret this rather obscure wording to mean that processing of personal data revealing political persuasion may take place where this is reasonable, because it is relevant to the appointment of a person to a public position (eg as mayor).

The prohibition on the processing of personal data revealing a person's membership of a trade union (*lidmaatschap van een vakbond*) does not apply where the processing is carried out by the particular trade union or the trade union federation to which the trade union belongs, provided that this is necessary for the aims of the trade union or the trade union federation. The personal data may not be disclosed to a third party without the consent of the data subject.[226]

v Personal data relating to health

The WBP only partly regulates the processing of data relating to health (*gezondheid*). The Medical Treatment and Information Act (Wet Geneeskundige Behandelingsovereenkomst[227]) also deals with the processing of medical data and conforms with the provisions of the Directive.[228]

The WBP makes the following exceptions to the prohibition on the processing of health data:[229]

First of all, medical professionals, health care institutions or facilities and social services may process health data, provided the processing is necessary for the proper treatment and care of the data subject,

226 WBP a 20.

227 *Stb* 1994 838. The Wet Geneeskundige Behandelingsovereenkomst regulates the agreement between a "hulpverlener" (a natural or juristic person providing medical help) and a patient, in terms of which the "hulpverlener" gives medical treatment to the patient. The Act also contains provisions as to how the file ("dossier") that the "hulpverlener" has on the patient should be kept, and as to the right of access of the patient to the file.

228 See WBP *Memorie van toelichting* 108.

229 The term "gezondheid" should be interpreted broadly to include data emanating from a medical check-up, as well as data relating to medical treatment. It should also be interpreted to refer to both physical and psychological health. Should a manager of an employee make a note that the employee is ill, that should also be considered to be health data, even if it does not reveal anything about the medical condition of the employee (see WBP *Memorie van toelichting* 109).

or for the administration[230] of the institution or professional practice concerned.[231] Other sensitive data, for example data relating to race, religious belief and sex life, may also be processed where it is necessary to supplement the processing of personal data concerning a person's health, with a view to the proper treatment or care of the data subject.[232]

Secondly, insurance institutions may process health data if this is necessary for assessing the risk to be carried by the insurance institution and the data subject has not objected to the processing,[233] or because processing is necessary for the performance of the insurance policy.[234]

Thirdly, schools may process health data, but only in restricted circumstances. They may process health data on pupils if this is necessary with a view to providing special support for pupils or making special arrangements in connection with their state of health.[235]

Fourthly, a probation and after-care institution, a particular probation officer, the Child Care and Probation Board, and guardianship and family supervision institutions may process health data in so far

230 Administration should be interpreted narrowly. It may include quality control of services provided by colleagues, as well as administration of accounts for the medical treatment. For other administrative purposes, data that are not identifiable should be used (WBP *Memorie van toelichting* 110).

231 WBP a 21(1)(a). The Directive provides that health data may be processed if this is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of health-care services (Dir 95/46/EC a 8(3)). The Dutch legislator chose a simpler formulation, but the intention is that the concepts "een goede behandeling of verzorging" (the proper treatment and care) and "het beheer van de betreffende instelling of beroepspraktijk" (for administration) include all the elements listed in the Directive (WBP *Memorie van toelichting* 110).

232 WBP a 21(3). It is possible eg that someone's race may be relevant in making a diagnosis, in which case such sensitive data may be processed. So, too, may someone's religious beliefs or sexual orientation be important in the psychological treatment of the person. See WBP *Memorie van toelichting* 115.

233 The data subjects should be informed of their right to object (see WBP a 33 as discussed in par 4.3.7).

234 WBP a 21(1)(b). More detailed rules may be issued by general administrative order (see WBP a 21(5)).

235 WBP a 21(1)(c). Eg, providing access to buildings for students in wheelchairs. Schools may therefore only process health data of students with special needs, eg handicapped students, and only in so far as this is necessary to achieve the two aims mentioned.

as this is necessary to perform their statutory duties.[236]

Fifthly, the Minister of Justice may process health data in so far as this is necessary in connection with the implementation of prison sentences or detention measures.[237]

Lastly, administrative bodies, employers or institutions working for them may process health data if this is necessary for the proper implementation of statutory provisions or collective agreements which create rights dependent on the state of health of the data subject.[238] They may also process such data if this is necessary for the reintegration of or support for workers or persons entitled to benefit in connection with illness or work incapacity.[239]

An important guarantee that applies in all of the above exemptions is that the **health data may only be processed by a person who is subject to a duty of confidentiality** because of official, professional or legal provisions, or because of an agreement. Where the responsible parties personally process data, and are not already subject to such a duty, the Act requires them to treat the data as confidential, except where they are required by law or in connection with their duties, to communicate such data to other parties who are authorised to process the data in terms of one of the exemptions already discussed.[240]

A special provision is included regarding the processing of data concerning *erfelijke eigenschappen*

236 WBP a 21(1)(ca). This article was introduced by the *Nota van wijziging Tweede kamer vergaderjaar* 1988–1999 25 892 nr 10 December 1998.

237 WBP a 21(1)(d). Eg, the health of the inmate may determine the diet that is prescribed, or the manner in which the inmate is transported (see WBP *Memorie van toelichting* 112).

238 Examples of these claims are payments due to inability to work, or other measures that have to be taken in terms of social security, eg adapting the data subject's house to accommodate a physical handicap. See also WBP *Memorie van toelichting* 113–114.

239 WBP a 21(1)(e). More detailed rules may be issued by general administrative order (see WBP a 21(5)). The employer's obligations in this area are also regulated by other legislation, eg Wet Terugdringing Ziekteversuim*Stb*. 1993 750; and Wet Uitbreiding Loonoorbetalingsplicht bij ziekte (*Stb* 1996 134) (see WBP *Memorie van toelichting* 113).

240 WBP a 21(2).

(inherited characteristics or **genetic data**). Such data may only be processed in so far as this processing takes place with respect to the data subject from whom the data have been obtained, unless a serious medical interest prevails, or the processing is necessary for the purpose of scientific research or statistics.[241] In other words, where persons furnish health data that may also affect other members of their families, such data may not be processed with respect to the other family members, since they did not supply it.[242]

vi Personal data relating to criminal offences

The prohibition on the processing of criminal data relating to a person (*strafrechtelijke persoonsgegevens*) does not apply where the processing is carried out by bodies charged by law with applying criminal law and by the responsible parties who have obtained these data in accordance with the Police Files Act (Wet Politieregisters[243]) or the Judicial Records and Certificates of Good Behaviour Act (Wet op de Justitiele Documentatie en op de Verklaringen omtrent het Gedrag[244]).[245]

Criminal data may also be processed by the responsible parties in order to protect themselves. They may process criminal data for their own purposes to assess applications by data subjects in order to

241 WBP a 21(4). In the case of processing of genetic data for scientific or statistical purposes, the provisions of a 23(1)(a) and 23(2) apply, ie the processing is only valid if the data subject has consented thereto (a 23(1)(a)) or if the special provisions for scientific research or statistical purposes are complied with (a 23(2) (see text to fn 206)).

242 The Dutch legislator wanted to negate the *uitstralingseffect* (radiation effect) that genetic data have. The Dutch Constitution in a 1 (non-discrimination clause) guarantees that everybody is equal; this principle may be undermined if genetic data can be used to classify people into two groups: those that are healthy and those that pose a certain risk (eg for insurance purposes). See WBP *Memorie van toelichting* 116.

243 *Stb* 1990 414. On this Act, see fn 116.

244 *Stb* 1955 395. On this Act, see Vunderink "Openbaarheid versus privacy" 212.

245 WBP a 22(1). This provision applies to the Department of Justice and its organs and special investigative services. It does not relate to the police force, since the general norms relating to their work have been dealt with in sectoral legislation, ie the Police Files Act (*Stb* 1990 414) (WBP *Memorie van toelichting* 120. Also see fn 116).

take a decision about them or to deliver a performance to them.[246] Processing of criminal data to protect controllers' interests, provided that this concerns criminal offences which have been or may be committed against them, or in their service, is also permitted.[247] The processing of these data concerning personnel of the responsible party must take place in accordance with the rules established in compliance with a procedure referred to in the Works Councils Act (Wet op de Ondernemingsraden[248]).[249]

Criminal data may also be processed in the interest of third parties who could become a victim of a criminal activity.[250] Such processing could be done if one of the following circumstances exists:

- The processing is done by a responsible party permitted to do so in terms of a licence issued under the Private Security Organisations and Investigation Bureaus Act (Wet Particuliere Beveiligingsorganisaties en Rechercheberaus).[251]

- The third parties are juristic persons forming part of the same group as referred to in article 2:24b of the Civil Code (Burgerlijk Wetboek).[252]

246 Eg, whether the responsible party wants to enter into a contract with the data subject. See WBP a 22(2)(a). These criminal data will mostly originate from court records or police files.

247 WBP a 22(2)(b). Criminal data of this type will mostly originate from the controllers' own records (WBP *Memorie van toelichting* 120).

248 *Stb* 1971 54.

249 WBP a 22(3). The provisions imply an instruction to self regulation (WBP *Memorie van toelichting* 121).

250 What the WBP has in mind in this article is the exchange of data by persons or institutions *inter se*. Criminal data that originate from the public sector (eg the police) are regulated by other Acts, eg the Police Files Act (Wet op Politieregisters) (see fn 116) or the Judicial Records and Certificates of Good Behaviour Act (Wet op de Justitiele Documentatie en op de Verklaringen omtrent het Gedrag) (*Stb* 1955 395) (see WBP *Memorie van toelichting* 121).

251 WBP a 22(4)(a). These private security companies may, with the permission of and under the supervision of the authorities, fulfil tasks that relate to the combatting of crime.

252 WBP a 22(4)(b). This exception makes it possible for institutions in the same field to exchange data that may relate to criminal activities of a data subject. An example would be where the Credit Registration Bureau, involved in the extension of credit by the banking sector, disseminates personal data relating to criminal

(continued...)

- ❒ Appropriate and specific guarantees have been provided and the procedure referred to in article 31 has been followed.[253]

Other sensitive data may also be processed together with the criminal data where this is necessary to supplement the processing of criminal data for the purposes for which these data are being processed.[254]

All the above provisions regarding criminal data are also applicable where the data relate to a ban imposed by the courts concerning unlawful or objectionable conduct.[255]

It should be noted that in terms of the Directive, if any derogations are made to the prohibition on the processing of criminal data by anyone other than an official authority, the Commission of the European Union must be notified.[256]

vii Personal data relating to sex life

No specific exemption is made for the processing of data relating to a person's sex life (*seksuele leven*), and such data may be processed only if they fall within the general exemption provided for by article 23, or where it is necessary to process such data in conjunction with other sensitive data in order to achieve the aim for which the other sensitive data are being processed.[257]

252(...continued)
activities of people who are applying for credit to its members. See WBP *Memorie van toelichting* 121.

253 WBP a 22(4)(c). A 31 provides that the data protection authority (the CBP) should make a prior investigation of the processing activities that will take place.

254 WBP a 22(5). An example would be where a charge of sexual harassment is laid by an employee against another employee. In such instances other sensitive personal data, eg relating to sex life, may also have to be processed. See WBP *Memorie van toelichting* 122.

255 WBP a 22(6).

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

257 See fn 232 and the text to fn 254.

4.3.5 Codes of conduct

The Directive on data protection encourages member states to draw up of codes of conduct for the various sectors that process data, with a view to contributing to the proper implementation of the national data protection provisions.[258] At the time of the adoption of the Directive the Netherlands was one of the few member countries whose existing data protection legislation already made provision for the establishment of codes of conduct.[259]

The WBP[260] provides that an organisation or organisations that plan to draw up a code of conduct[261] may request the data protection authority (the CBP) to declare that, given the particular features of the sector or sectors of society in which these organisations operate, the rules contained in the code accurately reflect the WBP or other legal provisions relating to the processing of personal data. If the code provides for the settlement of disputes concerning the observance of the code, the CBP may give such a declaration only if it has been provided with sufficient guarantees as regards independence. These provisions are likewise applicable to amendments of or extensions to existing codes of conduct.[262]

In other words, two factors need to be considered when testing a code of conduct: firstly it must be established that it correctly applies the data protection provision of all relevant legislation,[263] and secondly, the nature of the sector in which it will apply must be reflected. The purpose of a code of

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

259 The UK also had such provisions. See WBP *Memorie van toelichting* 129. According to Hustinx, the relevant provision in the Dutch data protection legislation served as a model for Dir 95/46/EC a 27 (Hustinx "The case of data protection" 285).

260 WBP a 25(1).

261 The term "code" should be interpreted broadly to include any form of collective self regulation with regard to the handling of personal data. Rules of conduct can also be considered a code of conduct (WBP *Memorie van toelichting* 130).

262 WBP a 25(2).

263 Not only the provisions of the WBP, but also all other legislative provisions regarding the processing of personal data need to be considered (see WBP *Memorie van toelichting* 129).

conduct must be to translate the legislative provisions into a practical application in the specific information sector involved. The code should be more than a repetition of the legislative provisions.[264]

The CBP may consider such an application only if in its opinion the persons making the request are sufficiently representative and the sector or sectors concerned are sufficiently precisely defined in the code.[265] The decision on such a request must be taken within a reasonable time, which may not be longer than thirteen weeks.[266]

The declaration applies for the duration of the code of conduct, but the period of application may not exceed five years from the date on which the declaration was announced. Where approval is requested for an amendment to an existing code for which a declaration has been issued previously, the amendment will apply for the duration of such a previous declaration.[267]

The CBP is responsible for publishing the declaration, together with the associated code, in the *Government Gazette*.[268] More detailed rules may be applied by general administrative order to a particular sector concerning the matters covered in articles 6 to 11 and 13.[269] The CBP must indicate

264 WBP *Memorie van toelichting* 130.

265 WBP a 25(3). The WPR a 15(2) also required that the code should have been drawn up after sufficient consultation with organisations of interested parties. This provision caused problems in practice and the WBP consequently does not have such a requirement. However, because it is required that the applicants should be representative of the sector concerned, the CBP will be able to refuse an application from a group that does not have the support of most of the organisations in that sector (WBP *Memorie van toelichting* 130).

266 WBP a 25(4). Such a decision is equivalent to a decision within the meaning of the General Administrative Law Act (Algemene Wet Bestuursrecht – AWB (*Stb* 315 1992)) and must be arrived at in accordance with a procedure laid down by a 3(4) of that Act. For information on the AWB, see fn 162.

267 WBP a 25(5). The legislator felt that a maximum period for which the code will be valid should be imposed, since the circumstances in a particular sector are bound to change. Similarly, many provisions entail a balancing of interests, and it is also possible that ideas on the correct weight that should be given to a particular interest may change. Where a maximum period is imposed, it means that the codes will be updated on a regular basis to adapt to changing circumstances and ideas (WBP *Memorie van toelichting* 131).

268 WBP a 25(8).

269 WBP a 26(1). These articles are discussed above in par 4.3.4.1.

in its annual report the extent to which it considers the implementation of this subarticle to be desirable.[270]

4.3.6 Notification to supervisory authority

As stated previously, the Directive requires of member states to provide that the data controller (in Dutch law called the responsible party), or its representative, should furnish certain information to the supervisory authority, that that particular information should be published in a register of processing operations, and that a prior investigation of certain processing operations should be carried out on the basis of this information.[271]

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 responsible party 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.[272]

4.3.6.1 Notification process

The responsible party must notify the CBP or the data protection officer (*functionaris*)[273] before carrying out any automated (or partly automated)[274] processing operation intended to serve a single

270 WBP a 26(2).

271 Dir 95/46/EC a 18–21.

272 WBP *Memorie van toelichting* 133. The importance of the transparency of processing is emphasised by Prins 1998 (1) *Priv & Inf* 11, 12.

273 The WBP permits an organisation to appoint a data protection officer to supervise, in an independent manner, the processing of personal data in order to ensure that the processing is done in accordance with the provisions of the Act. If an organisation chooses to appoint a data protection officer, this person can be notified instead of the CBP. See WBP a 62–64, and see par 4.3.11.2.

274 WBP a 27(1).

purpose or different related purposes.[275] 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.[276] The importance of the notification procedure is illustrated by the fact that noncompliance with this provision is punishable with a fine, or if it was intentional, or even with imprisonment for a maximum of six months.[277]

The responsible party should supply the following information to the supervisory authority:[278]

- the name and address of the responsible party[279]
- the purpose or purposes of the processing[280]
- a description of the categories of data subjects and of the data or categories of data relating thereto
- the recipients or categories of recipients to whom the data may be supplied[281]
- the planned transfers of data to countries outside the European Union[282]

275 WBP a 27(3). It is important to note that for the notification process the purposes need only be "related". This should not be confused with the material norm that requires the processing of data to be for a purpose that is "compatible" with the purpose for which data were collected. Ie, the responsible party need not notify the data protection authority about every separate processing activity, but may give one notification for several related processing activities (WBP *Memorie van toelichting* 133).

276 WBP a 27(2) and see par 4.3.6.3. The Directive leaves it to member states to apply the notification process to non-automated processing operations at their discretion (Dir 95/46/EC a 18(5)). The Dutch legislator felt that non-automated processing as a general rule does not pose a serious threat to the privacy of data subjects, and therefore thought it unnecessary that such processing be subject to notification. However, in those cases where a serious threat to privacy is posed, the processing activities should be investigated by the data protection authority prior to the processing, and in these exceptional situations it is also necessary that the notification procedure be complied with (WBP *Memorie van toelichting* 134–135).

277 See WBP a 75.

278 WBP a 28(1).

279 In case of an alleged unlawful use of personal data, this information would be needed to contact the responsible party (WBP *Memorie van toelichting* 136).

280 This determines the nature of the data processing and is the criterion against which the contact (*omgang*) with the personal data is tested (WBP *Memorie van toelichting* 136).

281 In the explanatory memorandum to the WBP, it is emphasised that the descriptions should give a very clear picture of who will receive the information: "De bedoeling is dat het helder en doorzichtig wordt hoe de gegevens worden verwerkt" (WBP *Memorie van toelichting* 138).

282 This provision reflects the origin of the WBP, namely the European Union Directive on data protection, and enables the government to fulfil it obligation, in terms of the Directive, to inform the European Commission

(continued...)

- a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing[283]

Processing of personal data can be lawful only if it is compatible with the purpose for which the data were originally collected,[284] and the notification must therefore also specify the purpose or purposes for which the data or categories of data were collected.[285] This means that where a notification is given of a multifunctional information system with diverse purposes, the different purposes for which the data were originally collected should be spelled out. The different uses that are made of the data should be tested for compatibility with the purposes for which the data were collected.[286]

The CBP or *functionaris* should be notified of a change in the name or the address of a responsible party within one week. Other changes in the notification which appear to be of more than incidental importance should be notified within one year of the previous notification.[287]

Any processing which represents a departure from the details given in the notification must be recorded and kept for at least three years.[288] More detailed rules on how the notification should take place may

282(...continued)
if a third country does not, in its opinion, provide an adequate level of protection of the rights of the individual. This provision enables the government to become aware of proposed transfers before they take place, and to determine the level of protection provided by such country (WBP *Memorie van toelichting* 137).

283 This description obviously cannot be very detailed, because that in itself would compromise security. Furthermore, for this reason, this information cannot be included in the register kept by the CBP and *functionaris* (see WBP a 30(1)) and is also not made known to third parties requesting information in terms of WBP a 30(3). On WBP a 30, see par 4.3.6.2.

284 WBP a 9, and see par 4.3.4.1.

285 WBP a 28(2).

286 WBP *Memorie van toelichting* 138.

287 The Directive requires of member states to specify the procedures to be followed to notify the supervisory authority of any changes in the information conveyed to them (Dir 95/46/EC a 19(2)).

288 WBP a 28(4).

be laid down by general administrative order.[289]

In a few instances, the Directive allows member states to **simplify** the notification procedure or **exempt** processing from it.[290] The WBP implements this by providing that by general administrative order, data processing which is unlikely to affect the fundamental rights and freedoms of the data subject adversely may be exempted from the notification requirement.[291] In such a case, the following particulars must be supplied: the purposes of the processing, the processed data or categories of processed data, the categories of data subjects, the recipients or categories of recipients to whom data are to be supplied, and the period during which the data are to be stored.[292]

Where this is necessary in order to trace criminal offences in a particular case, it may be laid down by general administrative order that the notification of processing by the responsible parties who are vested with investigative powers by law is exempt from notification. Compensatory guarantees 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.[293]

The notification requirement does not apply to public registers set up by law,[294] or to data supplied to

289 WBP a 28(5).

290 See ch 3 par 4.2.4.10 and Dir 95/46/EC a 18(2).

291 WBP a 29(1). Processing operations of this kind would be those that people would presumably be aware of because they take place so often. An example would be the processing of data in terms of the Archiefwet of 1995 (WBP *Memorie van toelichting* 140). Under the WPR, the following types of files were eg exempted fromregistration: book-keeping and financial administration systems, personnel and salary administration systems, administration systems relating to the internal management of organisations, subscription administration systems, membership and supporters administration systems, other personal data files to the extent that they contain no data other than names, addresses, domiciles, postal codes and similar data necessary for purposes of communication (see Nugter *Transborder flow of personal data* 154).

292 WBP a 29(2). By giving this information in the exemption order, the aim of transparency in the processing of personal data is met, but at the same time many controllers are relieved of the administrative burden of notification (see WBP *Memorie van toelichting* 140–141).

293 WBP a 29(3).

294 Examples of such registers are trade registers, matrimonial property registers and land registers (WBP (continued...)

an administrative body pursuant to a legal obligation.[295]

4.3.6.2 Publicising of processing operations

The data protection authority (the CBP) and the data protection officer (*functionaris*) must maintain an up-to-date register of the data processing reported to them. At a minimum, the information contained in the notification sent to them, except for the description of the security measures,[296] must be included in the register.[297] The register must be open to any person for inspection at no cost.[298] Where the processing is not subject to notification, the responsible party must make the relevant information available to any person who so requests,[299] 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.[300]

4.3.6.3 Prior investigation

The notification process enables the supervisory authority to carry out prior investigations on processing operations likely to present certain risks to the rights and freedoms of data subjects. The Directive

294(...continued)
Memorie van toelichting 24). Since these registers are published and open to the public, notification has in effect already taken place (see WBP *Memorie van toelichting* 142).

295 WBP a 29(4).

296 The security measures taken should be treated in confidence (see WBP *Memorie van toelichting* 137).

297 WBP a 30(1).

298 WBP a 30(2).

299 WBP a 30(3). Note that it is not required that the person should have an interest in the data or should be the data subject (WBP *Memorie van toelichting* 143). The responsible parties are not required to comply with this provision where this is necessary (a) in the interests of state security; (b) for the prevention, detection and pursuit of criminal offences; (c) for important economic and financial interests of the state and other public bodies; (d) for supervising compliance with legal provisions established for the interests referred to under (b) and (c); (e) for protecting the data subjects or the rights and freedoms of other persons (WBP a 43. On a 43, see par 4.3.9).

300 WBP a 30(4).

provides that member states may specify the risks in their legislation.[301] The WBP identifies three situations where the CBP[302] will have the authority to institute a prior investigation on processing activities, namely where the responsible parties intend to do one of the following:[303]

- process a personal identification number for a different purpose than the one for which it is specifically intended, with the aim of linking the data with data processed by other responsible parties, unless such use complies with article 24 (that is, such use is permitted either in terms of the Act instituting it or in terms of a general administrative order)[304]

- record data on the basis of their own observations without informing the data subjects thereof (this does not include public registers instituted by law)[305]

- process criminal data or data on unlawful or objectionable conduct on the behalf of third parties other than under the terms of a license issued under the Private Security Organisations and Investigation Bureaus Act (Wet Particuliere Beveiligingsorganisaties en Recherchebureaus) (The European Commission should be notified of this type of processing.)[306]

The WBP provides that prior investigations may also be required by law or general administrative order in the case of other types of data processing, where such processing carries particular risks for the individual rights and freedoms of data subjects.[307] The CBP must indicate in its annual reports the extent

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

302 In terms of the Directive, the data protection officer may also carry out the prior investigations, but the Dutch legislator decided to allow only the CBP to carry out the prior investigations (see WBP *Memorie van toelichting* 145).

303 WBP a 31(1)(a)–(c).

304 See text to fn 209.

305 WBP a 31(2).

306 WBP a 31(4).

307 This provision foresees the possibility that new technologies may develop that pose specific risks to (continued...)

to which, in its opinion, the provisions should be rendered applicable to such data.[308]

The responsible party should notify the CBP of data processing that could be subject to a prior investigation.[309] The responsible party should then suspend the processing activities until the prior investigation has been carried out, or until notice has been received from the CBP that a more detailed investigation will not be carried out.[310] However, this provision does not apply to processing activities already under way at the commencement of the WBP.[311]

The CBP must make its decision as to whether or not it will conduct a more detailed investigation within four weeks, and notify the responsible party in writing.[312] If the CBP decides to conduct a more detailed investigation, it must indicate the period of time within which it plans to conduct this investigation. This period must not exceed thirteen weeks.[313] The detailed investigation leads to a statement concerning the lawfulness of the data processing.[314] Such a decision is equivalent to a decision within the meaning of the General Administrative Law Act (Algemene Wet Bestuursrecht), and must be arrived at in accordance with a procedure laid down by article 3(4) of that Act.[315]

307(...continued)
privacy and thus necessitates a prior investigation of processing activities (WBP *Memorie van toelichting* 146).

308 WBP a 31(3).

309 WBP a 32(1).

310 WBP a 32(2).

311 WBP a 79(3).

312 WBP a 32(3).

313 WBP a 32(4).

314 WBP a 32(5). The prior investigation is therefore based on a lawfulness criterion (WBP *Memorie van toelichting* 144). The CBP reaches a non-binding decision on the lawfulness of the proposed processing (WBP *Memorie van toelichting* 148). However, the responsible party remains responsible for the lawfulness or not of the activities (WBP *Memorie van toelichting* 144).

315 WBP a 32(6). On the AWB, see fn 162.

4.3.7 Duty to inform data subject [316]

In compliance with the Directive,[317] the WBP also requires the responsible parties to provide the data subjects with information, both where the data are obtained from the data subjects themselves, and where the data are obtained in another manner.[318]

4.3.7.1 Scope of duty to inform

The data subjects must at least be informed of the identity of the responsible parties and the purposes of the processing for which the data are intended.[319] More detailed information must also be given, provided that, given the type of data, the circumstances in which they have been obtained or the use made thereof, this is necessary in order to guarantee, as regards the data subjects, that the processing is being carried out in a proper and careful manner.[320]

Where the personal data are to be obtained from data subjects, the information must be given prior to

316 The responsibility placed on the responsible parties to inform data subjects of the fact that processing of their data is taking place is an important instrument in making the processing transparent. Processing of personal data can only be lawful if it is done in a transparent manner. The extent of the duty to inform depends on what is necessary to guarantee fair processing (see WBP *Memorie van toelichting* 149).

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

318 WBP a 33 and a 34. An example of the obtaining of personal data about a data subject "in another manner" is where data are obtained from third parties, eg data on creditworthiness that are obtained from a credit information bureau, or where data are obtained through own observation (WBP *Memorie van toelichting* 149–150).

319 WBP a 33(2) and a 34(2). The manner in which the information is supplied depends on the nature of the contact, but it must be given in such a way that data subjects actually take note thereof. Eg, where the data subject has to complete a form in which personal data are called for, the required information must be given on the form, and the data subject should be required to sign the form to indicate that notice has been taken of the information. Where the contact is by telephone, the information must be given orally, or when the contact is electronic, the information must be given on the screen before the personal data are supplied (see WBP *Memorie van toelichting* 152).

320 WBP a 33(3) and a 34(3). Examples of situations where more detailed information should be given are where additional information, that is not really needed for the completion of the primary transaction (eg for statistical purposes), is requested; or where the data are obtained by linking existing data systems to generate new information (see WBP *Memorie van toelichting* 154).

obtaining the data, unless the data subjects are already acquainted with this information.[321] Where the data are not obtained from the data subjects, the information must be given at the time when the data relating to them are recorded, or when it is intended to supply the data to a third party, at the latest on the first occasion when the data are so supplied, unless the data subjects are already acquainted with this information.[322]

Where the data are not obtained from the data subjects themselves, the information need not be given to the data subjects if it appears to be impossible or would involve a disproportionate effort to provide the information to the data subjects.[323] In that case, the responsible parties are required to record the origin of the data.[324] The information need likewise not be given if the recording or provision of the data is required by law. In that case, the responsible parties must inform the data subjects, upon their request, about the legal provision which led to the recording or supply of the data.[325]

4.3.7.2 Exemptions from and restrictions on duty to inform

The WBP provides for exemptions from and restrictions on the duty to inform the data subject in the

321 WBP a 33(1). In the WPR the duty to inform the data subject did not exist where it could "reasonably have been expected" that the data subject knew about the processing. Despite a request by *inter alia* the Netherlands during the preparation of the Directive to include this more flexible standard, the Directive (Dir 95/46/EC a 10 and 11) does not use the term "reasonably" and the standard in the WBP is as a consequence stricter than that in the WPR (WBP *Memorie van toelichting* 150).

322 WBP a 34(1). Data subjects' conduct could also indicate that they are aware of the fact that their personal data are being processed. Eg, where persons book a tour through a touring operator, the operator may assume that the persons know that their personal data are being processed in order to make the necessary arrangements (WBP *Memorie van toelichting* 151).

323 The duty to inform the data subject is therefore not an absolute right. Whether the effort involved is "disproportionate" depends *inter alia* on whether there are other ways of supplying the data subject with adequate information, as well as the medium in which the responsible party could be assumed to reach the most data subjects (see WBP *Memorie van toelichting* 155).

324 WBP a 34(4). The Directive requires the member states to provide "appropriate safeguards" where an exception is made to the duty to inform the data subject (Dir 95/46/EC a 11(2)). The WBP complies with this requirement by providing that the responsible party must keep a record of from whom and in what manner the data were collected (see WBP *Memorie van toelichting* 156).

325 WBP a 34(5).Once more, this is to provide "appropriate safeguards" as required by the Directive (Dir 95/46/EC a 11(2)).

interests of state security; prevention, detection and pursuit of crime; important economic and financial interests of the state and other public bodies; the supervision of compliance with legal provisions established in the interests of the previously mentioned two interests; and the protection of the data subjects or the rights and freedoms of other persons.[326] Further, the responsible parties are not obliged to comply with the provisions that require them to inform data subjects of the processing of their data where the data were not collected from the data subjects themselves,[327] where such processing is carried out by institutions or services for the purposes of scientific research or statistics, and the necessary arrangements have been made to ensure that the personal data can only be used for statistical or scientific purposes,[328] and where personal data are processed which form part of archive records that have been transferred to an archive storage place in terms of the Archives Act (Archiefwet 1995).[329]

4.3.8 Data subjects' rights

The WBP, in compliance with the Directive, provides data subjects with the right to have access to their personal data, the right to request correction of such data, and the right to object to the processing of their data.

4.3.8.1 Right of access

The right of access can be divided into three separate rights, namely the right of data subjects 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 responsible parties must make sure that the identity

326 WBP a 43. See par 4.3.9.

327 Ie the provisions of WBP a 34.

328 WBP a 44(1). See par 4.3.9.

329 WBP a 44(2). See par 4.3.9.

of the person making the request is properly established.[330]

First, data subjects have the right, freely and at reasonable intervals, to request the responsible parties to inform them as to whether personal data relating to them are being processed. The responsible parties must inform the data subjects in writing (or in another medium if the interests of the person making the request so require),[331] within four weeks as to whether personal data relating to them are being processed.[332]

In the event of such data being processed, the data subjects have the right, secondly, to obtain a full and intelligible summary thereof, a definition of the purpose or purposes of the processing, information on the data categories to which the processing relates and on the recipients or categories of recipients, as well as any available information about the origin of the data.[333] Prior to the responsible parties providing the requested information, the responsible parties must give third parties an opportunity to express their views where such information contains data concerning them, unless this appears to be impossible or would involve a disproportionate effort.[334]

Thirdly, the responsible parties must provide data subjects with information concerning the underlying logic of the automated processing of the personal data relating to them if requested to do so.[335]

330 WBP a 37(2). In the case of minors under the age of sixteen, or persons placed under legal restraint, the request must be made by their legal representatives, and the information must be supplied to the legal representatives (WBP a 37(3)).

331 WBP a 37(1).

332 WBP a 35(1).

333 WBP a 35(2). The right of access is formulated as a two-stage procedure (first getting confirmation that personal data are being processed and secondly getting a summary of the personal data). The WPR also had a two stage procedure, but it was accepted that both requests could be made simultaneously (Nugter *Transborder flow of personal data* 157).

334 WBP a 35(3).

335 WBP a 35(4). However, this may not result in an infringement of the copyright of the author of the program (WBP *Memorie van toelichting* 159).

The WBP provides for **exemptions and restrictions** to the data subjects' right to access their personal data, in the interests of state security; for the prevention, detection and pursuit of crime; in the interests of important economic and financial interests of the state and other public bodies; for the supervision of compliance with legal provisions established in the interests of the previously mentioned two interests; and for the protection of the data subjects or the rights and freedoms of other persons.[336]

The responsible parties may also refuse to comply with requests for access where processing is carried out by institutions or services for the purposes of scientific research or statistics, and the necessary arrangements have been made to ensure that the personal data can only be used for statistical or scientific purposes.[337]

4.3.8.2 Right to request correction

Those persons who have been informed that personal data relating to them are being processed may request the responsible parties to correct, supplement, delete or screen such data if they are factually inaccurate, partly or wholly irrelevant to the purpose or purposes of the processing, or are being processed in any other way which infringes a legal provision. The request for correction must also include the modifications to be made.[338]

The responsible parties must inform the person making the request in writing (or in another medium if the interests of the person making the request so require),[339] within four weeks of receiving the request as to whether and, if so, to what extent, they are complying therewith. A refusal to do so must be accompanied by reasons.[340] The responsible parties must ensure that a decision to improve,

336 WBP a 43. See par 4.3.9.

337 WBP a 44(1).

338 WBP a 36(1).

339 WBP a 37(1).

340 WBP a 36(2).

supplement, delete or screen data is implemented as quickly as possible.[341] Where personal data have been recorded on a data medium to which no modifications can be made, such as CD-ROM or microfiche,[342] 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.[343]

These provisions do not apply to public registers set up by law where such law provides for a special procedure for correcting, supplementing, deleting or screening data.[344]

Responsible parties who have corrected, supplemented, deleted or screened personal data in response to a request of the data subject have an obligation as soon as possible to inform third parties to whom the data have previously been supplied about the correction, addition, deletion or screening, unless this appears to be impossible or would involve a disproportionate effort.[345] If requested to do so, the responsible parties must also notify the data subjects of the third parties to whom they have disclosed the information.[346]

The data subjects requesting the information may be required to pay for expenses incurred in providing

341 WBP a 36(3).

342 WBP *Memorie van toelichting* 160.

343 WBP a 36(4). The Dutch legislator recognises that it is undesirable that data subjects' rights should be restricted because of the medium used to store the personal data. However, it is also not desirable to prevent the use of certain data media. A proposed solution is to update the permanent medium 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. "Correctie behoeft dus niet in alle omstandigheden te betekenen dat de onjuist gebleken persoonsgegevens worden verwijderd of vernietigd." See WBP *Memorie van toelichting* 160.

344 WBP a 36(5).

345 WBP a 38(1). The wording of this provision indicates that a balancing of interests must take place. The nature of the correction also 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 not found guilty, will require that even third parties who received the information a long time ago should be traced. However, a mere correction in an address will not impose the same burden (WBP *Memorie van toelichting* 162).

346 WBP a 38(2).

such information, but the payment may not exceed an amount to be laid down by general administrative order.[347] The payment must be refunded if the responsible parties correct, supplement, delete or screen data at the request of data subjects, at the recommendation of the CBP or by order of the courts.[348]

4.3.8.3 Right to object to processing

As required by the Directive,[349] the WBP provides that data subjects have the right to object to certain processing activities.[350]

First of all, data subjects may object to processing where the data subject has not consented to the processing, but it takes place pursuant to articles 8(e) and 8(f) of the WBP.[351] In terms of these two articles, personal data may be processed where this is necessary for the performance of a public law duty by an administrative body, or where it is in the legitimate interests of the responsible party or of a third party to whom the data are disclosed. In both instances, a balancing of interests must take place.[352] In the process of finding a balance, the responsible parties can only consider those circumstances known to them. Since the responsible party may not be aware of the particular circumstances of the data subjects, the WBP allows data subjects to register their objections with the responsible party, at any time, based on their particular personal circumstances.[353] The responsible party must then re-evaluate the necessity for the processing. No particular form is prescribed for the

347 WBP a 39(1). Under the WPR the amount was 10 Gulder (WPB *Memorie van toelichting* 162).

348 WBP a 39(2).

349 Dir 95/46/EC a 14.

350 WBP a 40 and a 41. On the difference between the right to object granted by article 40 on the one hand and article 41 on the other, see fn 169. In articles 17(2)(b) and 18(b)(3), a right to object to the processing of sensitive personal data in specific situations is also granted (see par 4.3.4.2.b and fn 221.) See also Schreuders 1998 (2) *Priv & Inf* 52, 55.

351 WBP a 8 spells out the only six grounds on which data may legitimately be processed (see par 4.3.4.1).

352 WBP *Memorie van toelichting* 163.

353 WBP a 40(1).

objection.[354] The responsible party must decide within four weeks of receiving a notice of objection as to whether the objection is justified.[355] If the objection is justified, the responsible party must immediately stop the processing.[356] The data subject may be required to pay for expenses incurred in dealing with an objection, but the payment may not exceed an amount to be laid down by general administrative order, and must be refunded if the objection is found to be justified.[357] The right to object does not apply to public registers set up by law.[358]

The Directive requires that the right to object to the processing of data must also exist where data are processed for direct marketing purposes at no cost and without any obligation to give reasons.[359] The WBP implements this requirement by providing that where data are being processed in connection with the creation or maintenance of a direct relationship between the responsible party or a third party and the data subject, with a view to recruitment for commercial or charitable purposes,[360] the data subjects may register their objection to such processing with the responsible party at any time and at no cost to themselves.[361] If the data subjects object to such processing, the responsible party must immediately

354 WBP *Memorie van toelichting* 164.

355 A refusal of the objection is a decision in terms of the General Administrative Law Act (Algemene Wet Bestuursrecht (AWB) (*Stb* 315 1992)), a 3(4), and the data subject may use the remedies provided in that Act, ie objection (*beswaar*) and appeal (*beroep*). The data subject will have a right to compensation for damage in terms of the WBP a 49 (see par 4.3.10.1) only after a judge has decided that the data subject's objection should be upheld and the responsible party is continuing with the (unlawful) processing (WBP *Memorie van toelichting* 164. On the AWB, see fn 162).

356 WBP a 40(2).

357 WBP a 40(3).

358 WBP a 40(4).

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

360 The WBP therefore also includes fundraising for charitable purposes under the concept "direct marketing". Also see WBP *Memorie van toelichting* 164–167 for an extensive discussion of the concept of direct marketing and the situations where processing of personal data may be permitted for these purposes.

361 WBP a 41(1). The WBP uses an "opt-out" system as opposed to an "opt-in" system (see ch 3 par 4.2.4.7 on the meaning of these concepts). Ie, data subjects should register their objections if they do not want to be subjected to direct marketing. The Dutch legislator decided to put the burden on the data subjects to object, because a system where the responsible parties first have to ask the data subjects whether they could be included in processing for direct marketing purposes would have been too burdensome for the

(continued...)

put a stop to the processing.[362]

Responsible parties processing or planning to process personal data for direct marketing purposes must notify the data subjects of the possibility of registering an objection to such processing. The WBP distinguishes between the situation where the responsible parties do the processing themselves and where they supply the information to third parties who do the processing. In the first instance, the data subjects can be notified of the possibility of objecting every time a message is sent to the data subjects in this regard.[363] Where the responsible party intends to give the information to third parties or use it on behalf of third parties for direct marketing purposes, appropriate steps must be taken to notify the data subjects of the possibility of objecting. In such a case the notification must be made via a suitable newspaper,[364] or in some other appropriate form. Where the data are regularly used for direct marketing purposes, this notification should be done once a year.[365]

4.3.8.4 Right not to be subject to automated decisions

In compliance with the Directive,[366] the WBP provides that persons may not be subject to decisions to which legal consequences are attached 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

361(...continued)
responsible parties from a financial point of view (WBP *Memorie van toelichting* 168). Note, however, that where the personal data that will be processed for direct marketing purposes were obtained from another person or institution (the original responsible party), the new responsible party must comply with a 34 and inform the data subject of his or her identity and the purposes of the processing. Also, the processing for direct marketing purposes must of course be compatible with the original purpose for which the data were collected (WBP a 9).

362 WBP a 41(2). Data subjects need not give reasons for their objections. In this context, the objection of a data subject creates an irrebuttable presumption that the data subject's interest outweighs that of the responsible party (WBP *Memorie van toelichting* 167).

363 WBP a 41(4).

364 The WBP distinguishes between a *dag-, nieuws- of huis-aan-huisbladen* (WBP a 41(3)).

365 WBP a 41(3).

366 Dir 95/46/EC a 15. See ch 3 par 4.2.4.8.

intended to provide a picture of certain aspects of their personality.[367]

Two exceptions are made to this prohibition, namely where such decisions:

- have been taken in connection with the conclusion or execution of contracts, and the requests of the data subjects have been met, or appropriate measures have been taken to protect their legitimate interests[368] (which include giving the data subjects the opportunity to express their views on the decisions)[369]

- are based on a law in which measures are laid down for protecting the legitimate interests of data subjects[370]

The responsible parties must also inform the data subjects about the underlying logic of the automated processing of the data relating to them.[371]

---

367 WBP a 42(1). According to the WBP *Memorie van toelichting* 169, the underlying idea is that making a decision on a person based on only specific information is less likely to infringe a person's privacy than when, because of the amount of information available on a person, a more or less unique profile (*beeld*) of a person is formed on a certain aspect of that person. Examples of aspects on which a profile can be formed are job performance, creditworthiness or conduct. In such a situation a decision is made on a person based on the interpretation of divergent information. Human dignity requires that such a decision should be made by another person and not merely by an automated system: "Het profiel mag geen grond zijn voor besluitneming over de persoon zonder daadwerklijke menselijke tussenkomst." See WBP *Memorie van toelichting* 170.

368 WBP a 42(2)(a). This provision makes it possible, eg, for a person to be prevented from drawing money from an automatic teller machine because the computer has detected the person's name on a blacklist. However, the computer may not have the final say in such a situation, and appropriate measures should be taken to allow the person to state his or her case (WBP *Memorie van toelichting* 170). See also Berkvens & Prins "Van WPR naar WBP" 343.

369 WBP a 42(3).

370 WBP a 42(2)(b).

371 WBP a 42(4). See also fn 335.

4.3.9 Exceptions and restrictions

The WBP, following the Directive,[372] recognises that it is not possible to protect personal data in absolute terms, and therefore allows exceptions and restrictions to general rules. The responsible parties are therefore allowed not to apply certain principles or comply with certain duties.[373] Exceptions are allowed with regard to the principle of compatible use,[374] the general duty to inform all persons, irrespective of their interest, about the processing of personal data,[375] the duty to inform data subjects when their personal data are processed,[376] and the right of data subjects to have access to their personal data.[377]

Exceptions are allowed if this is necessary[378] in the interests of:

- ❒ state security
- ❒ the prevention, detection and pursuit of criminal offences
- ❒ important economic and financial interests of the state and other public bodies
- ❒ the supervision of compliance with legal provisions established in the interests of crime prevention or the supervision of economic and financial interests of the state or public bodies
- ❒ the protection of the data subjects or the rights and freedoms of other persons[379]

Where processing is carried out by institutions or services for the purposes of **scientific research or**

372 Dir 95/46/EC a 13.

373 The Act gives the responsible party the competence to make an exception; the Act does not impose an obligation that the exception should be made (Schreuders 1998 (2) *Priv & Inf* 52, 56).

374 WBP a 9 (see par 4.3.4.1).

375 WBP a 30(3) (see par 4.3.6.2 and fn 299).

376 WBP a 33 and 34 (see par 4.3.7).

377 WBP a 35 (see par 4.3.8.1).

378 On the necessity criterion, see fn 155.

379 WBP a 43.

statistics, and the necessary[380] arrangements have been made to ensure that the personal data can only be used for such purposes,[381] the responsible parties are also exempted from compliance with the provisions that require them to inform the data subjects of the processing of their data where the data were not collected from the data subjects themselves,[382] or with a request for access.[383]

Where personal data form part of **archive records** transferred to an archive storage place in terms of the Archives Act (Archiefwet 1995[384]), the responsible parties are not required to inform the data subjects of the processing[385] of their data.[386]

4.3.10 Remedies and sanctions

4.3.10.1 Remedies

The Directive prescribes that individuals are 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.[387]

---

380 The term "necessary" indicates that proportionality should exist between the interest of protecting personal data on the one hand, and the cost and effort involved in making the arrangements on the other (WBP *Memorie van toelichting* 173. Also see fn 155).

381 WBP a 44(1).

382 Ie the provisions of WBP a 34.

383 Ie the provisions of WBP a 35.

384 The Archives Act contains provisions regulating the manner in which interested parties will be informed about the manner in which the archival records will be dealt with. See WBP *Memorie van toelichting* 43–44 and 173–174 for a lengthy discussion of the issues concerning personal data in archival records.

385 WBP a 44(2). Processing in this case refers to the storage of data (WBP *Memorie van toelichting* 43–44).

386 The Directive does not make it possible to exclude archival records from all the provisions of the WBP. Only the data subject's right to be informed of the processing in terms of a 34 is excluded by a 44(2). In terms of a 29, archival records could also be excluded from the duty to notify the CBP (see fn 291).

387 Dir 95/46/EC a 22.

The WBP,[388] in compliance with the requirement of the Directive, provides for remedies in the case of a decision taken in response to:

- a request for information on the processing of personal data where such processing is not subject to notification[389]
- a request to access personal data[390]
- a request to correct, supplement, delete or screen data[391]
- a request for information about third parties to whom information has been provided[392]
- the registering of an objection to processing[393]

Where the decision was taken by an administrative body, the WBP provides that such decision must be deemed to be equivalent to a decision within the meaning of the General Administrative Law Act (Algemene Wet Bestuursrecht).[394] In other words, the remedies provided by that Act, namely objection (*beswaar*) and appeal (*beroep*), are available to the aggrieved party.[395]

Where the decision was taken by a body other than an administrative body, the aggrieved party[396] may apply to the district court with a written request that the responsible party be ordered to grant or reject such a request or to recognise or reject an objection.[397] The application must be submitted within six

388 WBP a 45 and a 46.

389 WBP a 30(3). See text to fn 299.

390 WBP a 35. See par 4.3.8.1.

391 WBP a 36. See par 4.3.8.2.

392 WBP a 38(2). See par 4.3.8.2.

393 WBP a 40 and 41. See par 4.3.8.3.

394 WBP a 45.

395 For more information on the AWB, see fn 162.

396 Not only the data subject, but also a third party can use this procedure (see WBP *Memorie van toelichting* 175).

397 WBP a 46(1).

weeks of receiving the reply from the responsible party. If the responsible party does not reply within the time limit, the application must be submitted within six weeks of the expiry of this time limit.[398] The court must find in favour of the request where the objection is well-founded. Before handing down a ruling, the court must, if necessary, give the parties concerned an opportunity to put forward their views.[399]

Prior to initiating the appeal or court procedures provided for above, the party concerned may apply to the CBP 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. In that case the appeal may still be lodged or the court proceedings still be initiated after the party concerned has received notice that consideration of the case has been completed.[400]

During the period when the appeal or court proceedings referred to above are being dealt with, the bodies responsible for dealing with the dispute may obtain the opinion of the CBP.[401]

The Directive also requires that individuals must 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.[402] The WBP therefore provides remedies for any person who has suffered harm as a consequence of acts which contravene the provisions of the WBP.[403] For harm that does not comprise damage to property, the injured party has the right to fair compensation.[404] In general, the responsible parties are liable for such loss or harm, but where this was incurred as a result of the actions

398 WBP a 46(2).

399 WBP a 46(3).

400 WBP a 47(1).

401 WBP a 47(2).

402 Dir 95/46/EC a 23(1).

403 WBP a 49(1).

404 WBP a 49(2).

of the processors, they will also be liable.[405] The responsible parties or processors may be exempted wholly or partially from this liability where they can prove that the harm cannot be attributed to them.[406] The burden of proof that they are not liable rests with the responsible parties.[407]

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.[408]

4.3.10.2 Sanctions

The Directive also requires the national data protection legislation to lay down the sanctions to be imposed in the event of infringement of its provisions.[409] The WBP provides for administrative measures of constraint (*bestuursdwang*), administrative fines and penal sanctions. The CBP is authorised to apply administrative measures of constraint where in its opinion the obligations imposed by the WBP are not being complied with.[410] The CBP can come to such a decision after a prior investigation has been completed,[411] or subsequent to an investigation in terms of its investigative powers.[412] An example of an administrative measure of constraint would be the requirement that the responsible party screen

405 WBP a 49(3). The responsible parties are always liable, even where the processing is done by processors. The responsible parties do of course have a right of recourse against the processors. The processors can, however, also be held liable directly by the claimants for their part of the damage (WBP *Memorie van toelichting* 176).

406 WBP a 49(4).

407 The WPR a 9 made provision for risk-liability, but this has been watered down in the WBP, (see WBP *Memorie van toelichting* 176) because the Directive (Dir 95/46/EC a 23(2)) allows for exemption from liability. Also see Holvast 1998 (1) *Priv & Inf* 4, 6.

408 WBP a 50(1).

409 Dir 95/46/EC a 24.

410 WBP a 65 and see WBP *Memorie van toelichting* 186.

411 See par 4.3.6.3.

412 WBP a 60. See par 4.3.11.1.

or delete personal data.[413]

In the event of responsible parties acting in contravention of the notification provisions[414] the CBP may require them to pay an administrative fine. However, a fine may not be imposed where the responsible parties can give a reasonable explanation as to why they cannot be regarded as being responsible for the infringement.[415]

Responsible parties may also be subjected to penal sanctions in the form of fines or imprisonment.[416] A fine,[417] or where the offence has been committed deliberately, imprisonment for a period of up to six months,[418] can be imposed for contravention of one of the following:

- the prohibition imposed on responsible parties not established in the European Union to process personal data in the Netherlands unless they designate a person or body in the Netherlands to act on their behalf[419]

- the provisions regarding the required notification to the CBP before the processing of personal data takes place[420]

- a prohibition issued by the Minister of Justice on the forwarding of personal information to a

413 WBP *Memorie van toelichting* 186. The exercise of the administrative measures of constraint is further regulated by the AWB. On the AWB see fn 162.

414 Under WBP a 27 (see par 4.3.6.1).

415 WBP a 66.

416 WBP a 75.

417 WBP a 75(1). These punishable offences are petty offences (WBP a 75(3)).

418 WBP a 75(2). These punishable offences are indictable offences (WBP a 75(3)).

419 WBP a 4(3) (see par 4.3.3.3).

420 WBP a 27 and 28. See par 4.3.6.1.

country outside the European Union[421]

In addition to the officials designated by the Code of Criminal Procedure,[422] the officials from the Secretariat of the CBP designated for this purpose by the Minister are also responsible for detecting the above-mentioned offences.[423]

4.3.11 Supervision

The Directive provides that each member state must establish one or more independent public authorities to monitor the application of the data protection provisions adopted pursuant to the Directive.[424] The powers and functions of the supervisory authorities must also be spelled out.[425] In certain circumstances, the Directive also permits a data protection official to take over some of the functions of the data protection authority, in order to avoid unsuitable administrative formalities.[426]

4.3.11.1 Supervision by data protection authority: College Bescherming Persoonsgegevens (CBP)

a Functions and powers of CBP

The WBP establishes an independent data protection authority entitled the College Bescherming Persoonsgegevens (Board for the Protection of Personal Data) with a remit to oversee, through its

421 WBP a 78(2)(a). See par 4.3.12.

422 Wetboek van Strafrecht a 141.

423 WBP a 75(4).

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

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

426 Dir 95/46/EC recitals par (49) and a 18(2).

members and officials,[427] the processing of personal data in accordance with legal provisions.[428] The CBP also oversees the processing of personal data in the Netherlands, where the processing takes place in accordance with the laws of another country of the European Union.[429]

Responsibility for the supervision of compliance with the WBP as referred to in the paragraph above rests with the members and extraordinary members of the CBP, the officials of the CBP Secretariat and the persons designated by decision of the CBP.[430]

The members and officials of the CBP who are responsible for the supervision of compliance with the WBP are authorised to enter a residence without the consent of the resident,[431] provided that they have the express and special authority of the CBP to exercise this power.[432] The CBP, in order to assist an official, may apply administrative measures of constraint.[433] The CBP also has an advisory function and the government is obliged to request its opinion on Bills and draft texts of general administrative regulations relating entirely or substantially to the processing of personal data.[434]

---

427 WBP a 61(1).

428 The supervisory function of the CBP is not restricted to the provisions of the WBP, but extends to other legislation, administrative regulations and other legal provisions in terms of which personal data are processed. Two types of legislation that are supplementary to the WBP can be identified: in the first type the protection of personal data of a specific nature is extensively dealt with, and the provisions of the WBP are excluded. The powers of the CBP are spelled out in the specific legislation itself. An example of this type is the Wet Gemeentelijke Basisadministratie Persoonsgegevens (Municipal Database (Personal Records) Act) (*Stb* 1994 494). On this Act, see also fn 117. The second type of legislation does not exclude the WBP, but only contains more specific rules for certain types of personal data. An example of this type of legislation is the Wet Geneeskundige Behandelingsovereenkomst (Medical Treatment and Information Act) (*Stb* 1994 837) (WBP *Memorie van toelichting* 177).

429 WBP a 51(1).

430 WBP a 61(1).

431 WBP a 61(2).

432 WBP a 61(3).

433 WBP a 61(4). WBP a 61(5) provides that no appeal is possible on the grounds of a duty of confidentiality, insofar as information or assistance is required in connection with the involvement of the CBP in the processing of personal data. Also see fn 185.

434 WBP a 51(2). On the advisory function of the CBP, see WBP *Memorie van toelichting* 178.

Apart from its supervisory and advisory functions, the CBP must also perform the tasks entrusted to it by law and treaty.[435] As required by the Directive,[436] the CBP acts independently in the performance of its tasks.[437]

b Appointment, remuneration and discharge of members of CBP

The CBP consists of a chairperson and two other members. In addition, extraordinary members may be appointed. When appointing extraordinary members, an attempt must be made to choose representatives of different sectors of society.[438] The chairperson must fulfil the requirements governing the appointment of district court judges.[439] All the members are appointed by royal decree, on the orders of the Minister of Justice. The chairperson is appointed for a six-year term and the other two members and the extraordinary members for a four-year term. The members may be reappointed immediately afterwards. They can be discharged by the Minister of Justice at their own request.[440] They are also discharged by royal decree, on the orders of the Minister, at the age of sixty-five.[441]

The chairperson and the two other members receive remuneration for their work. The extraordinary members receive a session fee. In all other matters, their legal position is governed by general administrative regulation.[442] The chairperson and the two other members may not, without the authorisation of the Minister of Justice, carry out any other remunerated work where the nature or scale

435 WBP a 51(1). The specific tasks of the CBP will be discussed hereunder in par d in more detail.

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

437 WBP a 51(2). The independence of the data protection authority is guaranteed by the fact it is an autonomous administrative body (see WBP *Memorie van toelichting* 27. Also see fn 440).

438 WBP a 53(1).

439 As laid down in a 48(l) of the Judicature Act (Wet op de Rechterlijke Organisatie) (WBP a 53(2)).

440 WBP a 53(3). The independence of the data protection authority is reflected in the provisions regarding appointment and discharge (WBP *Memorie van toelichting* 180).

441 WBP a 54(1)).

442 WBP a 55(1).

of this work is incompatible with their work for the CBP.[443]

c Administrative organisation of CBP

The CBP has a Secretariat, the officials of which are appointed, suspended and discharged by the Minister of Justice, on the orders of the chairperson.[444] The chairperson directs the work of the CBP and the Secretariat.[445] The CBP must adopt rules of procedure. The rules must include provisions relating to the financial management and administrative organisation of the CBP, as well as to the methods of work and procedures aimed at the proper performance of the different tasks.[446] The rules and any modifications thereto must be sent to the Minister as soon as possible for approval.[447]

The CBP is represented by the chairperson and the two other members or by one of these persons.[448] The members must allocate responsibilities among themselves and involve the extraordinary members in such responsibilities as much as possible.[449]

d Tasks or duties of CBP

Throughout the WBP, certain tasks or duties are assigned to the CBP. Examples of these duties are:

❒ the granting of exemptions to allow the processing of sensitive data on the grounds of important

443 WBP a 55(2).

444 WBP a 56(1).

445 WBP a 56(2).

446 WBP a 56(3).

447 WBP a 56(4).

448 WBP a 57(1).

449 WBP a 57(2).These members can contribute expertise in a specific sector, and also involve the community (see WBP *Memorie van toelichting* 180).

general interests, and the notification of the European Commission of such exemptions[450]

- declaring that a code of conduct drawn up for a specific sector adequately reflects the WBP[451]
- advising in its annual report on the use of general administrative regulations in particular sectors[452]
- maintaining an up-to-date register of data processing reported to it[453]
- initiating prior investigations, reporting on aspects of such investigations in its annual report, and notifying the European Commission of certain processing activities after such investigations[454]
- mediating in disputes between the responsible party and an aggrieved party, or giving an opinion on disputes to parties dealing with the disputes[455]
- consulting with the Minister of Justice on the issuing of permits for the forwarding of personal data to non-European Union member countries that do not provide any guarantees for an appropriate level of protection[456]

The following duties are specifically assigned to the CBP in the article dealing with its composition, functions, powers etcetera:

450 WBP a 23(1)(e) and 23(3). See par 4.3.4.2, 4.3.4.2.

451 WBP a 25(1). See par 4.3.5.

452 WBP a 26(2). See par 4.3.5.

453 WBP a 30(1). See par 4.3.6.2.

454 WBP a 31(1). See par 4.3.6.3.

455 WBP a 47. See par 4.3.10.1.

456 WBP a 77(2). See par 4.3.12.

❒ producing an annual report[457]

The CBP must produce an annual report before September on the activities, policy pursued in general and the effectiveness and efficiency of its mode of operation, in particular during the preceding calendar year. The report must be sent to the responsible Minister (the Minister of Justice[458]) and the data protection officers[459] and be made available to the general public.[460]

❒ providing the responsible Minister, upon request, with the information necessary for the performance of his or her duties[461]

The Minister may demand leave to inspect business data and records where this is necessary for the performance of his or her duties,[462] unless the CBP has obtained the information from third parties[463] on condition that it is kept confidential.[464]

❒ initiating an investigation on its own or at the request of an interested party to determine the manner in which the provisions of the WBP are applied to the processing of data[465]

The CBP must make known its preliminary findings to the responsible parties involved in the

457 WBP a 58.

458 WBP a 1(j).

459 Referred to in WBP a 62. See par 4.3.11.2.

460 WBP a 58.

461 WBP a 59(1).

462 The Minister is politically responsible for the CBP (see WBP *Memorie van toelichting* 181).

463 WBP a 1(g) defines a third party as any party other than the data subject, the responsible party, the processor, or any person coming under the direct authority of the responsible party, or the processor who is authorised to process personal data.

464 WBP a 59(3).

465 WBP a 60(1).

investigation, and must give them an opportunity to voice their opinions. If an Act is involved in the investigation, the relevant Minister must also be informed of the preliminary findings.[466]

In the case of an investigation initiated at the request of an interested party, the CBP must inform the party of its findings, unless providing such information would be incompatible with the purpose of the data processing or the nature of the personal data, or unless important interests of parties other than the person requesting the investigation, including the responsible party, would sustain disproportionate harm in consequence. In the event of the CBP deciding not to inform the interested party of its findings, it must furnish the party with such information as it deems appropriate.[467]

- providing assistance to the supervisory authorities of the other member states of the European Union, provided this is necessary for the performance of their work[468]

- maintaining an up-to-date list of registered data protection officers[469]

The CBP also has duties at the international level. For example, it is appointed as the responsible party in terms of the Council of Europe Convention,[470] and is the representative for the Netherlands in terms of the Schengen Agreement and the Europol Agreement.[471]

466 WBP a 60(1a)

467 WBP a 60(2).

468 WBP a 61(6).

469 WBP a 63(3).

470 See ch 3 par 3.2.9.

471 See WBP *Memorie van toelichting* 179.

4.3.11.2 Supervision by data protection officer

As previously indicated, the Directive permits the controller to appoint a data protection official to ensure the internal application of the national provisions introduced pursuant to the Directive.[472] The WBP implements this provision by providing that a responsible party, or an organisation to which responsible parties are affiliated, may appoint its own data protection officer to supervise the processing of personal data in that organisation.[473] However, the fact that a data protection officer has been appointed does not mean that the CBP's authority is excluded. The only function of the CBP that is exclusively taken over by the data protection officer is the receipt of notifications of processing.[474]

a Qualifications of data protection officer

The only persons who may be appointed as officers are natural persons who possess adequate knowledge to enable them to perform their duties and can be regarded as sufficiently reliable.[475]

"Adequate knowledge" relates to knowledge of the organisation, the data processing that takes place within the organisation, the interests involved in the processing, as well as knowledge of the privacy legislation that applies to the processing of personal data in that organisation.[476]

Whether a person is "sufficiently reliable" will depend on his or her ability to balance the interests of all parties involved in the data processing in an independent fashion, and to make careful and correct use

472 Dir 95/46/EC a 18(2). The data protection officer originated in German law (see Holvast 1998 (1) *Priv & Inf* 4, 6).

473 WBP a 62.

474 See WBP *Memorie van toelichting* 184–185. See par 4.3.6.1.

475 WBP a 63(1).

476 WBP *Memorie van toelichting* 184.

of his or her powers.[477]

b Independence of data protection officer

The Directive requires that data protection officers must be able to exercise their functions in complete independence.[478] The WBP therefore provides that data protection officers may not receive any instructions from the responsible party or organisation that appointed them with respect to the performance of their duties, and they may not sustain any disadvantage as a consequence of performing their duties. Responsible parties must also give officers the opportunity to perform their duties properly.[479] Before taking up their duties, the data protection officers must be registered with the CBP by the responsible party or organisation which appointed them. The CBP must maintain an up-to-date list of registered officers.[480]

c Duties, functions and powers of data protection officer

The Directive requires the data protection officers to ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.[481] The WBP therefore provides that officers have an obligation to treat as confidential any information disclosed to them in connection with a complaint or request by data subjects, unless said data subjects have given their consent to publication.[482]

The function of the data protection officers is to supervise the processing of personal data in accordance

477 WBP *Memorie van toelichting* 184.

478 Dir 95/46/EC recitals par (49) and a 18(2).

479 WBP a 63(2).

480 WBP a 63(3).

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

482 WBP a 63(4).

with the provisions laid down by and under the Act, or in accordance with a code of conduct drawn up in terms of the Act. This supervision covers the processing of personal data by the responsible party who has appointed the officer or by the responsible parties affiliated to the organisation which appointed the officer.[483]

The responsible party or organisation must ensure that officers have the equivalent authority to perform their duties, to that provided for in article 5(2) of the General Administrative Regulations Act (Awb).[484] Officers may submit recommendations to the responsible party with a view to improving the protection of the data being processed. In case of doubt, they must consult the CBP.[485] It is not required by the WBP that the data protection officer should produce an annual report, but the responsible party or organisation appointing the officer may require that.[486]

4.3.12 Data flows with countries outside European Union

The Directive prescribes in article 25 that member states must prohibit the transfer of personal data to nonmember countries that do not ensure an adequate level of data protection.[487] All the circumstances surrounding the data transfer must be taken into account when assessing the adequacy of the level of protection afforded by a third country. Certain factors are required to be given particular consideration.[488]

The WBP implements these provisions by providing that personal data which are subject to processing

483 WBP a 64(1) and (2).

484 Since the data protection officers are not appointed in terms of the Awb, their powers do not arise from this Act, but have to be granted to them by the persons appointing them. Data protection officers should, eg, have access to all systems where data are processed (WBP *Memorie van toelichting* 185).

485 WBP a 64(4).

486 WBP *Memorie van toelichting* 185–186.

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

488 Dir 95/46/EC a 25(2).

or intended for processing after they have been forwarded to a country outside the European Union may only be forwarded if, without prejudice to the legal provisions adopted, that country guarantees an appropriate level of protection (*passend beschermingsniveau*).[489] An assessment of the appropriateness of the level of protection must take account of the circumstances affecting a data forwarding operation or a category of data forwarding operations.[490] Account shall be taken in particular of the type of data, the purpose or purposes and duration of the planned processing or processing operations, the country of origin and the country of final destination, the general and sectoral legal provisions applicable in the nonmember country concerned, as well as the rules governing the business sector and the security measures applicable in these countries.[491] The Minister of Justice must notify the Commission of the European Communities of the cases in which, in his or her opinion, a nonmember country is not providing any guarantees for an appropriate level of protection.[492]

An operation or category of operations to forward personal data to a nonmember country which does not provide guarantees for an appropriate level of protection is not completely excluded, but is subject to additional rules.[493] Such operation may still take place, provided that one of the following criteria is met:[494]

- the data subjects have given their unequivocal consent[495] thereto
- the forwarding operation is necessary for the performance of a contract between the data

489 WBP a 76(1).

490 The issue is therefore not whether the country in question has adequate or appropriate data protection provisions in general, but whether in the particular case the data that are being transferred will have adequate protection (WBP *Memorie van toelichting* 193).

491 WBP a 76(2).

492 WBP a 78(1)(a).

493 WBP *Memorie van toelichting* 194.

494 WBP a 77(1)(a)–(f). These criteria are derived from the Directive and are also discussed in ch 3 par 4.2.7.

495 For the definition of "consent" see WBP a 1(i) and the text to fn 147.

subjects and the responsible parties, or for the implementation of precontractual measures which were taken in response to the data subjects' request and which are necessary for the conclusion of a contract[496]

- the forwarding operation is necessary for the conclusion or performance of a contract concluded or to be concluded between the responsible parties and third parties in the interests of the data subjects[497]

- the forwarding operation is necessary on account of an important general interest, or for the establishment, exercise or defence in law of any right[498]

- the forwarding operation is necessary to protect the vital interests of the data subjects[499]

- the forwarding operation has been carried out from a register set up by law or from a register which can be consulted by any person who can invoke a legitimate interest, provided that in the case concerned the legal requirements for consultation are met

The WBP also provides an emergency outlet for those cases where the above criteria prove to be

496 An example of such a situation is where the data subject has to make a payment in terms of his or her contractual obligations. It might not be possible to foresee where this payment will have to be transferred to in the ordinary run of the banking traffic (WBP *Memorie van toelichting* 194).

497 An example of such a situation is where an insurer wants to reinsure with an underwriter in another country, and as a result personal details of the data subject have to be transferred to the other country. The data subject has an interest in this transaction. Data cannot be transferred for direct marketing purposes, however, since such a transaction is not in the interests of the data subject (WBP *Memorie van toelichting* 194).

498 This may eg include the forwarding of personal data to a debt collecting agency established outside the European Union before the start of a legal procedure (WBP *Memorie van toelichting* 194–195).

499 An example of such a transfer is where medical data need to be urgently transferred to a third country from a member country where the data subject has previously been treated, because the data subject has become seriously ill while visiting the third country (Data Protection Working Party *Transfers of personal data to third countries* 19).

inadequate. The Minister of Justice may, after consulting the data protection authority,[500] issue a permit for a personal data forwarding operation or category of such forwarding operations to a nonmember country that does not provide any guarantees for an appropriate level of protection. The detailed rules required to protect the individual privacy and fundamental rights and freedoms of persons and to guarantee implementation of the associated rights should be attached to this permit.[501] The Minister of Justice must notify the Commission of the European Communities of the fact that a permit has been granted.[502] The notification must also be published in the *Government Gazette.*[503]

Where the Commission of the European Communities or the Council of the European Union has taken a decision with regard to the level of protection provided by a third country,[504] the Minister of Justice must give effect to this decision by laying down by ministerial ruling or by decision that

- ❒ forwarding to a country outside the European Union is prohibited
- ❒ a country outside the Union is considered to guarantee an appropriate level of protection
- ❒ a permit that was issued is withdrawn or modified

500 The Dutch legislator felt that it could not authorise the issue of permits to the CBP, but at the same time it felt that the expertise of the CBP should be used when issuing permits, because this will result in a better quality of decision-making (WBP *Memorie van toelichting* 195).

501 WBP a 77(2).

502 WBP a 78(1)(b).

503 WBP a 78(3).

504 WBP a 78(2). As seen in the chapter on the Directive (ch 3 par 4.2.7), member states and the Commission must inform each other of cases where, in their opinion, a third country does not ensure an adequate level of protection. Where the Commission finds that this is the case, member states must prevent any transfer of data of the same type to the country in question. The Commission is instructed to enter into negotiations with third countries that fall short on the adequacy provision, at the appropriate time, to remedy the situation. Upon conclusion of such negotiations, the Commission may find that the third country does ensure an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. In such an instance, member states must take the measures necessary to comply with the Commission's decision (Dir 95/46/EC aa 25(3)–(6)). The above provision implements this provision of the directive in the WBP.

4.3.13 Transitional and final provisions

4.3.13.1 Time allowed for implementation

The Directive allows countries three years in which to bring their national laws into compliance with the Directive. Once national legislation has been adopted pursuant to the Directive, data processing operations already under way must be brought into conformity with the national legislation within three years.[505] New processing operations must of course immediately comply with the new legislation.

The Dutch legislator decided on two terms for the implementation of the WBP. A distinction was made between the processing of "ordinary" personal data and that of sensitive personal data. The regime introduced for sensitive data is of a higher level than the previous regime under the WPR, and it was felt that a longer period of time should be allowed to the responsible parties to bring this type of processing into conformity with the Act.[506]

Data processing operations that do not involve sensitive personal data are required to be brought into conformity with the WBP and notified to the data protection authority or officer within a year. This time limit may be extended by general administrative regulation to a maximum of three years with respect to the notification requirement.[507]

The processing of sensitive data must comply with the WBP within three years. Where the processing of sensitive data was done with the consent of the data subject, it is not necessary to make another request for such consent[508] with respect to processing which has already taken place and which is

505 Dir 95/46/EC a 32(1) and (2).

506 WBP *Memorie van toelichting* 196.

507 WBP a 79(1).

508 See WBP a 23(1)(a) and par 4.3.4.2, 4.3.4.2.

necessary for the performance of contracts made prior to the date of commencement of the WBP.[509]

4.3.13.2 Periodical re-evaluation of WBP

In the light of the rapid developments in the field of information technology, it was decided that the WBP should be re-evaluated periodically.[510] Consequently, the Ministers of Justice and of the Interior are required to send a report to Parliament on the effectiveness and effects of the WBP in practice within five years of the coming into force of the Act.[511]

5 SUMMARY

In summary, it can be said that the right to privacy is protected in Dutch private law and under the Dutch Constitution. Data protection legislation is mandated by the Constitution. The general data protection legislation is the Wet Bescherming Persoonsgegevens of 2000 which also implements the provisions of the EU Directive on data protection. The WBP provides a valuable model for South Africa to follow, since it addresses all data protection issues in a clear and concise manner.

509 WBP a 79(2).

510 WBP *Memorie van toelichting* 197.

511 WBP a 80.