Thematic Legal Study on assessment of data protection measures and relevant institutions

Country report Netherlands

Report commissioned by the European Union Agency for Fundamental Rights (FRA)

Bert-Jaap Koops
Colette Cuijpers
Sjaak Nouwt
Arnold Roosendaal
Suad Cehajic

TILT - Tilburg Institute for Law, Technology, and Society

12 March 2009

Contents

Executive Summary

[1]. This report provides an overview of data protection legislation, instruments, and institutions in the Netherlands, and identifies major deficiencies and provides an assessment of the effectiveness of the instruments and institutions as emerging from national debates.

Data Protection Instruments

[2]. The major data protection instruments for the Netherlands are Art. 8 ECHR, Art. 10(2-3) of the Dutch Constitution, the EU Data Protection Directive 95/46/EC, and the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*, hereafter: DPA). The norms and rules embedded in these instruments are occasionally interpreted with reference to other international standards, like Convention 108 of the Council of Europe or the OECD Data Protection Guidelines. Moreover, additional or alternative rules apply to certain sectors (telecommunications, health care, social security, police, national security, municipal records) implemented in sectoral legislation. The legislation is supplemented by codes of conduct, many of which have been approved by the Data Protection Authority (*College Bescherming Persoonsgegevens*, CBP). The CBP has also published practical guidelines, like an audit framework, to help organisations implement data protection rules.

Data Protection Institutions

[3]. The major data protection institution is the CBP, which supervises compliance with the various data protection laws. It has a wide remit, comprising advising – upon consultation or its own initiative – on draft legislation and administrative measures, testing codes of conduct, and enforcement, which entails various investigation and coercive powers, but also mediation, handling of complaints, and deciding upon processing sensitive data and data transfers to third countries. In 2007, the CBP shifted priorities away from advice and awareness-raising to pay more attention to enforcement. However, despite a recommendation by an official committee (*Commissie-Brouwer*) to attribute supervision and advice to different supervisory institutions, the CBP still adheres to combining both types of tasks. The CBP's budget was raised from € 6 mln to € 7 mln in 2008, but according to the CBP, this is still insufficient to ensure effective fulfillment of all its tasks. Other data protection institutions include

the various sectoral supervisors that enforce the sectoral laws and rules, along with arbitration committees supervising codes of conduct. Public and private organisations can also appoint an internal supervisor, the data protection officer (*functionaris voor de gegevensbescherming*); in 2007, there were 240 such officers.

Compliance

[4]. Few data are available about the compliance with the data protection legislation in practice. In 1995, the evaluation of the DPA's predecessor, the Data Registries Act, found significant gaps in compliance with the details and letter of the law, but overall reasonably adequate compliance with the spirit of the law. Persons responsible for maintaining data registries were often careful and conscientious in their handling of personal data, often intuitively complying with general data protection principles. It is not unlikely that the empirical evaluation of the DPA, currently in progress, will yield similar findings.

Sanctions

[5]. Three types of sanctions can be applied in case of an infringement of data protection law: administrative enforcement actions (*bestuursdwang*), administrative fines (*bestuurlijke boete*), and penal sanctions. A non-official sanction occasionally applied in practice is negative publicity. Administrative enforcement sanctions can be imposed for all breaches of data protection law; administrative or penal fines can be imposed for violations of notification duties; intentional violations have higher sanctions than non-intentional ones. Sanctions are seldom imposed, however: 2006 yielded three administrative fines, and 2007 39 penalties imposed on a daily basis in case of non-compliance (*dwangsom*). Penal sanctions have not been imposed so far. Given the recent shift towards enforcement, the CBP might perhaps impose more sanctions in the future.

Awareness

[6]. The few data available on people's awareness of data protection rights and obligations indicate that many rights and obligations do not seem to be exercised due to lack of familiarity with the rules, both with the public and with small and medium enterprises and lower government

organisations. Surveys of privacy awareness show that citizens are generally aware of privacy issues and attach some or considerable importance to privacy protection, but that they easily disclose personal data. This is caused not so much by trust that data will be processed correctly, but by feelings of inevitability and resignation that data have to be provided. Citizens have considerably more trust in data processing by the government than by private parties. Nevertheless, one survey found that 43% of respondents thought the government should do more to protect their privacy.

Deficiencies

[7]. The DPA is currently being evaluated. The first stage (2007) consisted of a literature study, the second (yet to appear) of empirical research. As appears from the first stage evaluation, several deficiencies can be observed. Lack of clarity and vagueness of the statutory concepts and open terminology is seen as a major deficiency, for example, how the concepts of 'personal data' and 'controller' should be interpreted, also in light of technological developments. Another issue is the general, comprehensive character of the DPA, which leads to complexity and inflexibility of the act. Moreover, the DPA is very procedural in nature and provides few substantive standards. It is questioned whether drafting codes of conduct, as stimulated by the DPA, has sufficient added value. Rules on transfer to third countries are seen as problematic for transfers to third-country offices of data controllers themselves. Data protection legislation also entails substantial administrative burdens for organisations, which perhaps should be reduced.

[8]. Other deficiencies relate to the Data Protection Authority (CBP), which seems to receive too little funding to fulfil its various tasks adequately. Lack of funding might perhaps also be seen as an indirect steering instrument for the government, thus raising doubts on the true independence of the supervisory authority. Similarly, it is questioned whether data protection officers can be really independent in practice. Various scholars also argue that the CBP should have more sanctioning powers.

Effectiveness

[9]. Several of these deficiencies seem to result in a lack of effectiveness of data protection legislation. As with the predecessor of the DPA, the Data Registries Act, the legislation is said to be too complicated to

work with in practice, and rules seem often not to be translated into daily practice at the workfloor. Overall, the DPA seems to provide insufficient guidance for controllers and data subjects to realise their rights and duties in practical contexts. Moreover, in court cases, the legislation is often ineffective, both due to difficulties in proving damage and to a lack of attaching proper consequences to privacy infringements of privacy. Finally, the literature questions the future-proofness of the data protection system in light of technological developments, such as profiling and ambient technologies.

Solutions

[10]. Solutions to improve the deficiences and enhance effectiveness are proposed in the area of strenghtening the funding and powers of the supervisory authority, giving greater priority to strict enforcement and sanctioning violations, raising awareness of data protection rules and of the importance of protecting privacy, and providing more concrete guidance at the workfloor, for example with the six principles outlined by the Brouwer Committee. Moreover, at the EU level, the Data Protection Directive should be revised to address the problems of complexity, vagueness, and technological developments.

1. Overview

[11]. This report provides an overview of data protection in the Netherlands. It has been written as a country report for a thematic study commissioned by the European Union Agency for Fundamental Rights (FRA). The study's goal is a comparative assessment of effectiveness of data protection measures and relevant institutions in the EU. This country report is based on desk research of official and academic literature, supplemented with information provided upon our request by the Dutch Data Protection Authority (CBP). The study was conducted in December 2008 and January 2009; the text of the report was finalised on 12 March 2009.

[12]. The report is structured on the basis of a questionnaire provided by FRA. In this Chapter, we provide a general overview of data protection legislation, instruments, and institutions, and indicate major deficiencies and an assessment of the effectiveness of the instruments and institutions as emerging from national debates. In the following Chapters, we describe more in-depth the role of the Data Protection Authority, compliance issues, sanctions, privacy awareness, other deficiencies, and good practices.

1.1. Constitutional and international standards

[13]. Data protection in the Netherlands is enshrined in various domains of the law and other regulatory instruments. We first give an overview of constitutional (Dutch Constitution 1983) and international (EU, CoE, UN, OECD) standards, followed in the next section by national data protection instruments.

Dutch Constitution (1983)

[14]. Article 10 of the Dutch Constitution, introduced during the revision of the Constitution in 1983, embodies the right to privacy (para. 1) and data protection (paras. 2-3). Subsection 1 of this article stipulates that everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to an act of the Dutch parliament. Further, subsection 2 indicates that rules to protect privacy shall be laid down by an act of the parliament in connection with the recording and dissemination of personal data. Finally, subsection 3 stipulates that rules concerning the rights of persons to be

informed of data recorded concerning them and of the use that is made thereof, and to have such data connected shall be laid down by an act of the parliament.[1]

European Union

[15]. For Dutch legal practice, Directive 95/46/EC is the most relevant instrument within EU law.[2] This Directive has been implemented in the Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens, Wbp*), while Directive 2002/58/EC[3] has been implemented in the Telecommunications Act (*Telecommunicatiewet, TW*). A Bill to implement Directive 2006/24/EC[4] in the Telecommunications Act is currently awaiting approval by the First Chamber. Besides these Directives, articles 7 and 8 of the Charter of Fundamental Rights of the European Union[5] are also slowly gaining in importance in legal practice.

Council of Europe

[16]. The most important instrument for privacy protection is Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), including the case law of the European Court on Human Rights, on the protection of privacy and private life. Also relevant is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[6] although the EU Data Protection Directive plays a more direct role in safeguarding data protection in the Netherlands. Other Council of Europe instruments of some relevance are:

- The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Dataflow (2001).

[1] See http://www.minbzk.nl/contents/pages/6156/grondwet_UK_6-02.pdf, last consulted 07.02.2009.
[2] Directive 95/46/EC of 24 October 1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995, p. 31.
[3] Directive 2002/58/EC of 12 July 2002 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. (Directive on privacy and electronic communications), OJ L 201 of 31.07.2002, p. 37.
[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ L 105/54 of 15.03.2006 and amending Directive 2002/58/EC.
[5] Charter of Fundamental Rights of the European Union, Official Journal of the European Communities C 364/1, 18.12.2000.
[6] ETS 108, January 1981, also known as the Treaty of Strasbourg or Convention 108.

- The Convention on Human Rights and Biomedicine (1997), especially its Article 10 on 'Private life and right to information'.
- Basic Principles contained in the Appendix to the Recommendation Rec(87)15 of the Committee of Ministers to Member States Regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987, at the 401st meeting of the Ministers' Deputies.

UN instruments

[17]. Of some relevance, but in practice somewhat less than the EU and CoE instruments, are privacy safeguards in UN instruments, in particular article 12 of The Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights (ICCPR, 1966), General Comment No. 16 on Article 17 ICCPR (especially its paragraph 10 on personal data), and the Guidelines for the Regulation of Computerized Personal Data Files adopted by a resolution of the General Assembly of the United Nations on the 14th December 1990.

OECD instruments

[18]. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980) have been influential in the Dutch thinking about data protection, particularly in combination with the subsequent establishment of the data protection principles in CoE and EU law. Also relevant to mention is the Declaration on Transborder Data Flows (11 April 1985).

1.2. Dutch data protection instruments

Legislation

[19]. With respect to the Dutch data protection legislation, a distinction can be made between specific data protection legislation and general data protection legislation. The former is to be found in fields such as telecommunications (Telecommunications Act (*Telecommunicatie-wet*)), health care (Medical Treatment Contracts Act implemented in the Dutch Civil Code (*Wet op geneeskundige behandelings-overeenkomst*)), and social security (Work and Social Assistance Act (*Wet Werk en Bijstand*)). Please note that general data protection legislation, i.e. the Personal Data Protection Act, is not applicable if one of the five specific data protection acts is applicable. For instance, if in a certain case the Police Data Act (*Wet politiegegevens*) is

applicable, then the Personal Data Protection Act is excluded from application.

[20]. The general data protection instrument, applicable both to the public and private sector, is the Personal Data Protection Act (*Wet Bescherming Persoonsgegevens (Wbp)*).[7] This was enacted in 2000 and entered into force on 1 September 2001.[8] One of the central features of the Act, the duty to notify the Data Protection Authority of articles 27 and 28, is further regulated in the Notification Decree (*Meldingsbesluit Wbp*);[9] several types of processing are exempted from this notification duty through the Exemption Decree (*Vrijstellingsbesluit Wbp*).[10]

[21]. For specific sectors, other data protection regimes apply:

- Intelligence and Security Services Act (*Wet op de inlichtingen- en veiligheidsdiensten 2002* (*Wivd*));
- Municipal Personal Records Database Act (*Wet gemeentelijke basisadministratie persoonsgegevens* (*Wet GBA*));
- Police Data Act (*Wet politiegegevens (Wpg)*);
- Judicial Data and Criminal Records Act (*Wet justitiële en strafvorderlijke gegevens* (*Wjsg*));
- Electoral Act (chapter D) (*Kieswet, hoofdstuk D*).

Codes of conduct and Guidelines

[22]. The Dutch government promotes self-regulation by organisations that process personal data. Self-regulation has been made possible legally in article 25 of the Personal Data Protection Act. This is mainly effectuated through code of conduct instruments (*Gedragscodes*) and practical guidelines (*Praktische handreikingen*). The practical guidelines differ from code of conduct instruments as the former can be seen as audit products which organizations can use to verify their position regarding the protection of personal data within their organisation. Furthermore, Codes of Conduct have to be approved by the Dutch Data Protection Authority in order to be legally valid.

[23]. The following following Codes of Conduct have been approved:[11]

- Code of Conduct for Private Detective Offices (*Gedragscode voor particuliere recherchebureaus*)

[7] *Staatsblad* [Dutch Official Journal] 2000, 302.
[8] Decree of 5 July 2001, *Staatsblad* 2001, 337.
[9] *Staatsblad* 2001, 244.
[10] *Staatsblad* 2001, 250.
[11] The approved Code of Conduct instruments can be consulted in Dutch at http://www.cbpweb.nl/indexen/ind_wetten_zelfr_gedr.shtml, last consulted 07.02.2009.

- Code of Conduct for the Recruitment and Selection Industry (*Gedragscode voor de werving & selectiebranche*)
- Code of Conduct on the Processing of Personal Data by the Dutch Business Information Offices (*Gedragscode inzake verwerken van persoonsgegevens van de Nederlandse Vereniging van Handelsinformatiebureaus*)
- Code of Conduct for Court Bailiffs (*Gedragscode voor Gerechtdeurwaarders*)
- Code of Conduct on the Use of Personal Data in Scientific Research (*Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek*)
- Code of Conduct for Medical Scientific Research (*Gedragscode voor gezondheidsonderzoek*)
- Code of Conduct on the Use of Personal Data in Research and Statistics (*Gedragscode voor verwerking van persoonsgegevens bij onderzoek en statistiek*)
- Code of Conduct for the Pharmaceutical Industry (*Gedragscode voor de farmaceutische industrie*). The validity of this code expired on 4 September 2007 and has yet to be approved by the Data Protection Authority for another term.
- Code of Conduct for Banks and Insurance Companies (*Gedragscode voor banken en (zorg)verzekeraars*). The validity of this code expired on February 5 2008 and has yet to be approved by the Data Protection Authority for another term.

[24]. Several practical guidelines have been developed by the Data Protection Authority. These can be found on the website of the Data Protection Authority as 'Compliance Tools'. The Dutch DPA website describes them as follows:[12]

- *Quickscan*: The Quickscan is a list with 13 questions regarding privacy protection in the organisation. The questionnaire is chiefly intended to create awareness about privacy protection within an organisation. The results of the Quickscan only give an overall picture of the status of the privacy protection in an organisation. The questionnaire can be completed by every employee in an organisation. The web site contains a detailed explanation to the possible answers for the Quickscan. On the basis of this explanation, the person completing the list can assess what the meaning of the answers given to the questions is and what follow-up actions can be undertaken.
- *Data Protection Act Self-evaluation*: The Data Protection Act Self-evaluation is an instrument for the management of organisations to obtain an opinion about the implementation of

[12] See http://www.dutchdpa.nl/indexen/en_ind_wetten_zelfr_compliance.shtml, last consulted 07.02.2009.

and/or compliance with the provisions of the Wbp. The Data Protection Act Self-evaluation should be conducted by officers that are familiar with the Wbp and with the ICT facilities in the organisation. The provisions of the Wbp have been conveniently arranged into nine primary questions. For each primary question, the organisation should determine its ambition level and arrive at a factual assessment. The confrontation of factual assessment and ambition level will then provide an understanding of the status in the domain of protecting personal data within the organisation. The primary questions are supported by dozens of questions that the organisation can use to independently conduct the Data Protection Act Self-evaluation. If desired, management can decide to have the self-evaluation (independently) reviewed. In this way, the instrument will be more valuable for the organisation. The Data Protection Act Self-evaluation has been set up in accordance with the INK model. The document describes the steps that the organisation can use to effectively and efficiently conduct the Data Protection Act Self-Evaluation.

- *Privacy Audit Framework*: The Privacy Audit Framework has been drawn up so that a privacy audit can be conducted within an organisation by a certified auditor. The Framework also starts from nine clusters of areas of attention. The outcome of a privacy audit will provide the management with a high degree of certainty regarding the status of the protection of the personal data in the organisation. The decision to have a privacy audit conducted should be well considered. Such an audit is rather costly and is only useful if the organisation is ready for this. Early consultation with the company accountant is thus recommended.[13]

1.3. Relevant institutions

[25]. Several institutions in the Netherlands are concerned with data protection. General supervision over a number of data protection acts is assigned to the Dutch Data Protection Authority (*College Bescherming Persoonsgegevens* (*CBP*)). The CBP supervises the compliance with and application of the Personal Data Protection Act, the Police Data Act and the Municipal Personal Records Database Act. The CBP is bound by the standards laid down in the General Administrative Law Act (*Algemene wet bestuursrecht* (*Awb*)).[14]

[13] See http://www.dutchdpa.nl/indexen/en_ind_wetten_zelfr_compliance.shtml, last consulted 07.02.2009.

[14] See http://www.dutchdpa.nl/, last consulted 07.02.2009. For the Dutch website, see http://www.cbpweb.nl/, last consulted 07.02.2009.

[26]. The Personal Data Protection Act provides the opportunity for public and private organisations that process personal data to appoint their own internal supervisor, the data protection officer (*Functionaris voor de Gegevensbescherming* (*FG*)).

[27]. Next to the national supervisor there are also sectorial supervisors concerned with specific data protection acts governing specific industries. Furthermore, there are also arbitration committees concerned with the supervision of specific code of conduct instruments. Please note that the brief descriptions of the institutions presented below have been adopted from their respective websites.

- Health Care Inspectorate (*Inspectie voor de Gezondheid* (*IGZ*)). The Netherlands Health Care Inspectorate protects and promotes health and healthcare by ensuring that care providers, care institutions and companies comply with laws and regulations. The inspectorate makes impartial decisions and reports on request and at its own initiative to the Minister of Health, Welfare and Sport. Recently, in co-operation with the CBP, the inspectorate published a report on (the lack of) information security in Dutch hospitals.[15] The Health Care Inspectorate acts in the public interest and concentrates mostly on problems that members of the public are unable to assess or influence themselves. People must be able to rely on the quality and safety of care and products. The mission focuses on patient safety, effective care and care that is patient orientated.[16]
- Independent Post and Telecommunications Authority (*Onafhankelijke Post en Telecommunicatie Autoriteit* (*OPTA*)). OPTA is a governmental body and non-departmental agency of the Ministry of Economic Affairs that operates as an Autonomous Administrative Authority (*zelfstandig bestuursorgaan)*. OPTA independently regulates compliance with legislation and regulations in the areas of post and electronic communications. The legislation and regulations are intended to promote competition on these markets, resulting in more choice and fair prices for consumers. OPTA can also impose fines on distributors of spam or adware and spyware.[17]
- National Ombudsman (*Nationale Ombudsman*). The institution of National Ombudsman is established in order to give individuals an opportunity to place complaints about the practices of government before an independent and expert body. The mechanism works alongside existing institutions, such as Parliament, the courts, and internal complaints procedures.

[15] *Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm*. Report available in Dutch at: http://www.igz.nl/publicaties/rapporten/2008/informatiebeveiliging, last consulted 07.02.2009.
[16] See http://www.igz.nl/uk/, last consulted 07.02.2009.
[17] See http://www.opta.nl/asp/en/, last consulted 07.02.2009.

Applying to the Ombudsman may result in steps being taken in particular cases, and, in a broader context, help to restore public confidence in government. The National Ombudsman also formulates decisions in data protection cases with regard to administrative authorities.[18]

- Appeal Committee of the Association of Private Security Organisations (*Beroepscommissie van de Vereniging van Particuliere Beveiligingsorganisaties*) has been established in connection with the Code of Conduct for Private Detective Offices.
- Supervision Council (*Raad van Toezicht*) has been established in connection with the Code of Conduct on the Employment of Personal Data by the Dutch Business Information Offices.
- Chamber of Court Bailiffs (*Kamer van Gerechtsdeurwaarders*) has been employed in connection with the Code of Conduct for Court Bailiffs.
- Complaints Committee (*Klachtencommissie*) has been employed in connection with the Code of Conduct for Medical Scientific Research.
- Committee of Supervision (*Commissie van Toezicht*) has been employed in connection with the Code of Conduct for the Recruitment and Selection Industry.

1.4. Deficiencies and effectiveness

[28]. The main questions related to the deficiencies and effectiveness of the Dutch data protection system will be dealt with in this section. First the matter of deficiencies will be explored by giving a summary of deficiencies observed in the literature. Second, the debate about the effectiveness of the data protection system will be addressed.

[29]. Article 80 of the Personal Data Protection Act states that within five years from the entry into force of this act, the Dutch government has to present a report to the Dutch parliament on the effectiveness and effects of this act in practice. This evaluation of the Dutch DPA has been conducted in two stages. The first stage of the evaluation, a literature study, was concluded in 2007 and presented in the report *First Phase of the Evaluation of the Personal Data Protection Act* (*Eerste fase evaluatie Wet bescherming persoonsgegevens*).[19] The

[18] See http://www.ombudsman.nl/english/ombudsman/the_institution/introduction.asp, last consulted 07.02.2009.

[19] See G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009. An English summary can be consulted at page 207 of the report.

findings and conclusions drawn in this report are used below for answering the questions regarding the deficiencies and effectiveness of the data protection system in the Netherlands. The second stage of the evaluation consists of case studies and interviews, concerning the effectiveness of the Personal Data Protection Act in practice. The report was published on 16 February 2009;[20] since the report was published after our research period (see above, para. 11), we have been able to include only its main conclusions in this country report.

Deficiencies

[30]. Our inquiry on deficiencies has been conducted on the basis of extensive literature study. According to the first stage evaluation report, the lack of clarity and vagueness of the statutory concepts and open terminology is seen as a major deficiency, especially when interpreting relevant key terms and definitions. One example of confusion concerning the meaning and scope of key terms relates to the concept of personal data. Discussions regarding the scope of this concept have not only been raised from a general perspective – 'What are personal data, actually?'[21] – but also from specific perspectives, e.g., in relation to IP addresses.[22] As a result, the much strived for enhancement of transparency can be hindered. Moreover, the lack of clarity and vagueness will impede compliance with the law and may obstruct technological development and innovation.[23]

[31]. In the literature, further reference is made to deficiencies arising from the general, comprehensive character of the act.[24] In particular this concerns the complexity and inflexibility of the act. In addition, deficiencies are observed in literature concerning the determination of which person is the controller to whom the substantive standards of the law are primarily applicable. It is argued that these problems occur particularly in joint-venture constructions and in the context of the internet. According to some authors the act has a one-sided, procedural character and does not provide sufficiently firm substantive

[20] H.B. Winter et al. (2008), *Wat niet weet wat niet deert*, WODC 2008, http://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bescherming-persoonsgegevens-wbp-2e-fase.aspx#, last consulted 10.03.2009. (Note that the report is officially dated 2008, but was not published until February 2009.)

[21] J.M.A. Berkvens (2005), 'Persoonsgegevens wat zijn dat?', *Privacy en Informatie*, p. 258-259.

[22] College Bescherming Persoonsgegevens, 'Een IP-adres is niet altijd een persoonsgegeven', 19 March 2001, http://www.cbpweb.nl/documenten/uit_z2000-0340.stm, last consulted 07.02.2009.

[23] G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009, p. 208.

[24] *Privacy & Informatie* 2005 (6), special issue on the evaluation of the Dutch DPA.

standards.[25] In the same respect, other authors argue that the act is too unpractical because it assumes that each processing is tested against the open, but vague, standards of the act. In addition, they also criticise the designation of a whole category of data as special data (e.g. data on race and religion) leading to deficiencies because the sensitivity of special data depends on the context.[26]

[32]. With regard to the legally facilitated option to draft codes of conduct (article 25 of the act), some authors point at the time-consuming and expensive process in drafting them, concluding that they do not have many concrete advantages.[27] The literature is further questioning the issue whether a data protection officer can be truly deemed to be independent. With respect to the data protection authority, discussions have emerged whether this authority has sufficient (or insufficient) powers.

[33]. In the literature the deficiencies with respect to the compliance with the act and deficiencies in the field of enforcement are emphasised. Particular criticisms are aimed at the system of legal protection that provokes forum shopping due to the multiple receptive administrative and civil-law dispute resolution systems. Moreover, the multiple legal competences may also affect the unity of the law.

[34]. With respect to the international transfer of personal data,[28] especially the permit requirement[29] is experienced as a deficiency. This particularly applies to the transfer of personal data from an establishment of a controller within the EU to an establishment of the controller outside the EU. This 'internal' transfer does not fall under the exceptions and has to be considered a transfer to a third country.

Effectiveness

[25] G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009, p. 208.

[26] G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009, p. 208.

[27] G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009, p. 208.

[28] See, generally, D. Alonso Blas (2003), *Nota derde landen. De doorgifte van persoonsgegevens naar derde landen in het kader van de Wbp College Bescherming Persoonsgegevens*, February 2003.

[29] The Dutch Minister of Justice, after consulting the Data Protection Authority, may issue a permit for a personal data transfer or category of transfer to a non-member country that does not provide guarantees for an adequate level of protection.

[35]. The final conclusions from the first stage evaluation of the DPA[30] are divided into three aspects: legal aspects, enforcement and compliance, and awareness and familiarity. The authors of the first stage evaluation report present conclusions for each perspective on the question to what extent the objectives set by the Dutch and EU legislation are fulfilled.

[36]. First, the authors conclude that the *legal aspects* contain the most important deficiencies, arising from the difficult connection of the act with the Dutch legal system. The layered and compartmented system for the protection of personal data has become very complex and sometimes tends to overregulation. In addition, the conceptual system and set of instruments of the act are too abstract and leave too much space for interpretation to form a clear framework for assessing concrete questions and situations. As a result, the objective of providing a conceptual system that can be used for shaping legal rights and duties and for weighing interests is not fully realized.[31]

[37]. Second, from the perspective of *enforcement and compliance*, the unilateral character of the enforcement is pointed out, which mainly emphasises the administrative law process that is usually followed. In addition, the intended system of checks and balances is only shaped to a limited extent because of a lack of factual legal review of the principles from the act. Furthermore, self-regulation within the scope of the act leaves much to be desired, according to the report. It can also be concluded that particularly the objectives of the legal review of the powers granted to the Data Protection Authority and the further interpretation of substantive standards through self-regulation have only been realised to a limited extent.[32] Moreover, various authors have pointed out that the investigation and sanctioning powers of the CBP require strengthening; the CBP itself is also of the opinion that it needs a wider range of sanctioning powers, including the power to impose a fine for substantive violations.[33]

[38]. Another aspect influencing compliance and effectiveness of data protection regulation is administrative burdens. Several studies have analysed the administrative burdens resulting from Dutch privacy

[30] G. Zwenne et al. (2007), op.cit. n. 19.

[31] G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009, p. 210.

[32] G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009, pp. 210-211.

[33] P. De Hert (2009), *Citizens' data and technology. An optimistic perspective*, Den Haag, CBP, p. 39; J. Nouwt (2005), 'Tijd voor een nieuw punitief sluitstuk in de WBP?', *Privacy & Informatie* 2005(6), pp. 253-257; Personal communication from the CBP, 13 February 2009. See also below, § [46].

legislation and the (possibly negative) effects of these on the effectiveness of this legislation.[34] Actal, an official advisory body on red-tape reduction, issued a study regarding the problem of administrative burdens in privacy law,[35] but their recommendations to change the DPA have, to date, not been followed up.

[39]. Third, from the perspective of *awareness and familiarity*, it is striking that many rights and obligations of controllers and stakeholders that arise from the act are not effectively exercised through a lack of familiarity with these rights and obligations. As a result, one of the central objectives of the act, i.e. increasing the transparency of data processing through the granting of rights and obligations and the introduction of a regulatory authority, appear to have been (partly) unrealised.[36]

2. Data Protection Authority

[40]. The Dutch Data Protection Authority (*College bescherming persoonsgegevens: CBP*) supervises the compliance with acts that regulate the processing of personal data: the Personal Data Protection Act (*Wet bescherming persoonsgegevens: Wbp*), the Police Data Act (*Wet politiegegevens: Wpg*), and the Municipal Personal Records Database Act (*Wet gemeentelijke basisadministratie persoons-gegevens: Wgba*). The framework for performing this task has been set forth in the Wbp and other related legislation. The main legal basis for the CBP is Chapter 9 of the Dutch DPA. Articles 51-61 stipulate the tasks, powers, composition, and functioning of the CBP. With these provisions, the legislator has implemented Article 28 of the Data Protection Directive 95/46/EC, which requires the existence of such a supervisory authority that can fulfil its task completely independently.

[34] CBP, *Tien voorstellen voor administratieve lastenverlichting*, 7 December 2004, http://www.cbpweb.nl/documenten/med_20041207_alv.shtml, last consulted 07.02.2009; CBP, *Voorstellen wijziging Wbp*, 12 July 2005, z2004-1494; Projectgroep Wet Bescherming Persoonsgegevens, *Lasten van de Wbp. Rapportage aan de Commissie Administratieve Lasten*, Den Haag, 19 April 1999; C.M.K.C. Cuijpers (2006), *Verschillen tussen de Wbp en Richtlijn 95/46/EG en de invloed op de administratieve lasten- en regeldruk*, Tilburg: UvT; G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009, p. 90.

[35] J.J. Boog et al. (2006), *Administratieve lasten in het privacydomein. Reductievoorstellen nader bekeken*, Zoetermeer, http://actal.openims.com/actal_sites/objects/watdoetactal/Privacy/default66fb.pdf, last consulted 07.02.2009.

[36] G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009, p. 211.

Tasks and powers

[41]. The tasks and powers of the CBP correspond completely to the requirements of art. 28 of the Data Protection Directive.[37] Specifically, the tasks and powers of the CBP are:[38]

- Making recommendations regarding legislation;
- Testing codes of conduct;
- Testing regulations;
- Notification and preliminary examination;
- Information;
- Exemption from the prohibition to process sensitive data;
- Making recommendations regarding permits for transfers to third countries;
- International affairs (informal relations) and tasks (formal obligations);
- Mediation and handling of complaints;
- Official investigation;
- Enforcement.

Remit

[42]. The remit of the CBP is twofold. First, to supervise processing of personal data in accordance with the law; this includes supervising personal data processing in the Netherlands, if the processing takes place in accordance with the law of another EU country (art. 51 para. 1 Dutch DPA). Second, to advise on parliamentary Bills and draft Orders in Council that completely or substantially involve personal data processing (art. 51 para. 2 Dutch DPA).

[43]. As the CBP website indicates, its tasks sometimes relate to obligations, but as a rule they relate to powers. Subject to the law and the opinion of the court, the CBP is entitled to take decisions itself regarding the execution of these powers. Other tasks, such as providing information and conducting studies of new developments, result from the general supervisory task. The CBP has considerable free rein to work out the details of its tasks within the frameworks of the act and to set the necessary priorities and decide where to lay particular emphasis.[39]

[44]. In 2007, the CBP decided to change its policy, shifting priorities with respect to their various tasks. Rather than focusing on policy advice and awareness-raising, the CBP now gives priority to enforcement as

[37] Personal communication from the CBP, 13 February 2009.
[38] See http://www.dutchdpa.nl/indexen/en_ind_cbp.shtml, last consulted 07.02.2009.
[39] See http://www.dutchdpa.nl/indexen/en_ind_cbp.shtml, last consulted 07.02.2009.

its main supervisory task. Following this change of policy, the CBP has also had to make changes in its organisation by strengthening its investigative skills and their legal competence.[40]

[45]. The Committee Brouwer, which advised in January 2009 on the balance between security and privacy (see in more detail section 8), recommended that the tasks of the supervisory authority should be separated. An external supervisor can only effectively and credibly supervise compliance with data protection legislation if it has a 'free hand' and does not have to 'carry out tasks like giving advice, information, or facilitation'.[41] The CBP, however, stressed that, in their opinion, supervision and advice on law and policy should be done by a single authority, also in view of art. 28 of the Data Protection Directive.[42]

[46]. It can be doubted whether the CBP has sufficient powers to ensure effective data protection. In practice, data controllers do not seem to see the CBP's powers as a deterrent factor in their data processing practices, contrary to other supervisory authorities, like the OPTA or NMa (Netherlands Competition Authority), who have more powers to give higher fines. The fine for not notifying the processing of personal data to the CBP is a mere € 4,500. In the literature, also based on the observation that other European countries already have more powers for enforcement by criminal law, it has been suggested that the CBP could need more powers for the enforcement of data protection legislation by criminal procedures.[43] The CBP itself is also of the opinion that it needs a wider range of sanctioning powers, including the power to impose a fine for substantive violations.[44]

Relationship with the Article 29 Working Party

[47]. The article 29 Working Party is an independent advisory body and consultation organ of European data protection authorities. Its most important task, in the view of the CBP, is to promote and stimulate a

[40] CBP Annual Report 2007, p. 46 (in Dutch).
[41] Commissie veiligheid en persoonlijke levenssfeer (2009), *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer* [Do it simply – simply do it, to protect security and privacy], The Hague, January 2009, http://www.minbzk.nl/116513/rapport-'gewoon-doen, last consulted 07.02.2009.
[42] CBP, Press release, 22 January 2009, http://www.cbpweb.nl/documenten/pv_20090122_commissie_brouwer.shtml, last consulted 07.02.2009.
[43] J. Nouwt & T. Schudelaro (2006), *Hij die gegevens misbruikt wordt gestraft…,* Den Haag: Sdu, ITeR series Vol. 78; J. Nouwt (2005), 'Tijd voor een nieuw punitief sluitstuk in de WBP?', *Privacy & Informatie* 2005(6), pp. 253-257.
[44] Personal communication from the CBP, 13 February 2009.

uniform interpretation and application of the data protection principles of Directive 95/46/EC.[45]

[48]. The Opinions of the Working Party are considered by the CBP as 'very important, guiding documents, in particular when interpreting the Data Protection Directive'.[46] Although they are guiding (*richtinggevend*) rather than directly binding, they are very influential in the CBP's decisions and policy-making, in which they function as a source of law. This appears from the CBP's rules on requests for opinions (*verzoek om een zienswijze*) on new or unanswered legal problems concerning data protection issues; such a request will only be accepted by the CBP if the question can not be answered on the basis of existing legal sources. These legal sources include legislation, case-law, judgements by the CBP or its predecessor (the Registratiekamer), and Opinions of the Article 29 Working Party.[47]

[49]. The CBP is actively involved in the Article 29 Working Party. In 2007, it was represented in the following sub-groups:

- Justice, Freedom and Security (JLS);
- Employment;
- Contracts & Binding Corporate Rules;
- Internet Task Force;
- PNR;
- Personal Data & RFID.

[50]. The importance that the CBP attaches to the Article 29 Working Party's activities and achievements is visible, for example, from the CBP's annual report of 2007.[48] Mention is made in this respect of the serious discussions on the proposal by the European Commission, following the PNR agreement with the United States, to collect passenger data within the EU, and the SWIFT case. Reports in the media indicated that SWIFT stores back-up data on account holders in the United States and that the authorities in the US can demand access to these data. Contrary to their obligation in this respect, banks had not informed their customers of this fact. In a WP29 context, following coordinated action by all national data protection authorities, SWIFT indicated that it would open a data storage office in Switzerland in 2009, as such resolving the problem of the provision of data on inter-European transfers to the US. An active role of the CBP is also

[45] http://www.cbpweb.nl/indexen/ind_cbpint_art29.shtml, last consulted 07.02.2009.
[46] Personal communication from the CBP, 13 February 2009.
[47] CBP, *Regels voor het verzoek om een zienswijze*, 11 March 2008, http://www.cbpweb.nl/downloads_organisatie/Regels_voor_een_verzoek_om_een_zienswijze.pdf?refer=true&theme=purple, last consulted 07.02.2009.
[48] CBP, *Jaarverslag 2007*, http://www.cbpweb.nl/downloads_jaarverslagen/jv2007.pdf?refer=true&theme=purple, last consulted 07.02.2009.

claimed with regard to the Opinion of the Article 29 Working Party concerning the scope of the concept of 'personal data' and in view of strengthening the code of conduct for online marketeers (joined in FEDMA) with respect to minors. The annual report also states that the CBP regularly takes part in the joint supervisory data protection authority activities at an EU level in relation to collaboration between the police and judicial authorities. Altogether, according to the CBP, the Article 29 Working Party is the most important forum for discussion within the first pillar of the European Union.

Independence

[51]. The CBP is officially independent: article 52 para. 2 Dutch DPA stipulates that the CBP fulfils its tasks independently. The legal position of the CBP therefore seems to be sufficiently independent, at least in theory.

[52]. The CBP's independence in practice, however, has sometimes been questioned. The Committee Brouwer recommended to separate the enforcement task from the advisory task of the supervisory authority, since the advisory task does not allow a 'free hand' in supervision; the CBP itself does not consider this to be a restriction of its independence (see above, para. [45]). It has also been questioned in the literature whether in practice, the CBP can function truly independently from the government given its financial dependence. Observing that the supervisory authority has been financed for many years by the government in a very reserved (i.e., limited) manner, one scholar has argued that the government is indirectly influencing the scope and quality of the advice and supervision of the CBP.[49]

Budget and staffing

[53]. According to the Dutch DPA's Annual Report 2007, its staff consisted of 75 fte in 2007; about a third of these worked in supporting services, the rest operated in the primary processes of supervision, advice, and its other tasks. In 2007, the CBP had a financial budget of about € 6 mln. Besides, the CBP also had the revenues of fines and penalties that were paid, to an amount of € 20,300.[50] As a result of a resolution in the Dutch Parliament, the Minister of Justice decided to raise the CBP's budget for the year 2008 with € 1 mln.

[54]. On August 8, 2007, the CBP published a memorandum about its policy and budget 2008-2013. With this memorandum, the CBP informed the public that it will spend more capacity on the control and

[49] J.E.J. Prins (2007), 'Doeltreffend privacytoezicht', *Nederlands Juristenblad* 82(28), p. 1727.
[50] CBP Annual Report 2007, p. 54 (in Dutch).

enforcement of data protection legislation. As a result, the CBP announced that it will spend less capacity in advising citizens, industry, and government about data protection. The memorandum observes that to truly live up to its responsibility, the CBP needs a doubling of its budget within the next five years.[51] In that light, the raising of the budget with € 1 mln does not seem sufficient to ensure effective fulfillment of all tasks allocated to the CBP.

Powers to investigate

[55]. For *enforcement* purposes, according to article 60 Dutch DPA, the CBP can initiate an investigation into the manner in which the provisions laid down by or under the Act are being applied with respect to the processing of personal data. They can do this in cases where citizens lodge a complaint. An example is the case of alarmed parents who complained about Digidoor, an internet service in Almere that collected personal data about pupils from primary schools. The CBP concluded that the primary schools should better inform these pupils' parents about the collection, use, and distribution of their children's personal data.[52] In other cases, the CBP will start investigations on its own initiative. An example is the case of the transfer of passenger data by airline companies to the USA. In a letter, the CBP pointed out to airline companies flying to the USA and travel agencies that they have an obligation to inform their customers about the transfer of their personal data to the American authorities.[53] In this context, the CBP can also perform privacy audits. However, because article 60 provides the CBP with a discretionary power, the CBP can also decide not to initiate an investigation, despite a request by an interested party.[54]

[56]. The CBP's power to investigate includes the power of:

- ordering delivery of information;
- ordering to be given access to business data and documents;
- copying data and documents;
- entering dwellings without the inhabitants' consent;
- entering any other place and seizing the necessary equipment;
- access to those places with help of the police;
- being accompanied by persons appointed by the CBP;

[51] See http://www.cbpweb.nl/documenten/med_20070808_beleidbudget.shtml?refer=true&theme=purple, last consulted 07.02.2009.

[52] College bescherming persoonsgegevens, Scholen moeten ouders beter informeren (z2004-1152, 28 May 2005).

[53] College bescherming persoonsgegevens, Verstrekking passagiersgegevens door luchtvaartmaatschappijen aan VS (z2003-0239, 27 February 2003).

[54] Nationale Ombudsman, 4 August 2006, report number 2006/264.

- investigating things and taking samples;
- investigating means of transport, including their cargo and the related official documents.[55]

[57]. In specific cases, the CBP can initiate investigations and give its opinion about a planned processing of personal data (article 31 Dutch DPA). The investigations start after notification of the planned processing. The processing operations have to be suspended as long as the investigations take place or until the processor receives notice from the CBP that no more detailed investigations will be conducted (article 32(2) Dutch DPA).

Monitoring role

[58]. The CBP monitors the compliance with data protection legislation by using multiple sources of information. From citizens and data processors, it receives written and oral questions, announcements, complaints, requests for mediation or preliminary investigations, and other information, all of which can be used by the CBP as indications of potential violations of data protection rules. Moreover, the CBP performs investigations of its own initiative, and it also receives information from investigations by other supervisory authorities (like OPTA for the telecommunications sector) and occasionally other official authorities. All of this information is combined with the CBP's own knowledge of the field, and processed into an 'information analysis' and a yearly risk assessment.[56]

Advisory role

[59]. As to its *advisory task*, article 51, para. 2 Dutch DPA prescribes that the CBP has to be consulted on draft legislation and administrative measures that entirely or substantially relate to the processing of personal data. Usually, the CBP is consulted for advice on draft regulations by the government. It is also frequently being asked to give advice on draft legislation by the Second or First Chamber of Parliament. Those legislative recommendations are published on the CBP's website.[57] In some cases, for example in the case of the draft General Provisions of Environments Bill, the CBP advises on its own initiative.[58]

[55] C. Cuijpers (2003), 'Het College Bescherming Persoonsgegevens', In: C. Cuijpers et al (eds), *Privacy concerns. Het delen van persoonsgegevens bij fusies, overnames en binnen concerns*, NVvIR, Elsevier, p. 93.
[56] Personal communication from the CBP, 13 February 2009.
[57] http://www.cbpweb.nl/indexen/ind_publ_adv.shtml, last consulted 07.02.2009.(in Dutch).
[58] http://www.cbpweb.nl/downloads_adv/z2007-00304.pdf?refer=true&theme=purple, last consulted 07.02.2009. (in Dutch).

[60]. With respect to *testing codes of conduct*, the CBP can provide a declaration of agreement for a Code of Conduct. However, according to article 25 Dutch DPA, the declaration of agreement is not binding, but can be characterised as an expert's advice to the judge.[59] The same goes for decisions on prior investigations. These are also not legally binding, and must be characterised as an advice. It could be argued that it would be preferable if both types of decisions (on the Code of Conduct and prior investigations) were binding, from the perspectives of legal certainty, effectiveness, and legal protection, because no administrative procedure exists for these non-binding decisions by the CBP.

Publicity and awareness-raising role

[61]. The CBP tries to enhance awareness of privacy and data protection by actively communicating the results of its supervisory activities – both investigations and advice – via the media and its own website. Moreover, it publishes various types of practical guidelines on its website (see above, para. [22] and following). Thus, most of the decisions, opinions, and other documents published by the CBP are available to the public. They are published on the website of the CBP at www.cbpweb.nl. The CBP has also initiated Mijnprivacy.nl (*myprivacy.nl*), which contains questions and answers for Dutch citizens about the protection of their personal data.

3. Compliance

[62]. As to compliance with rules about processing *sensitive data*, with one exception (see below), the Dutch DPA has no possibility to request approval for processing special categories of personal data (sensitive data). A data controller who wants to process sensitive data will have to comply with the special conditions for processing these data (articles 16-23 of the Personal Data Protection Act). When no exemption in articles 17-22 can be found to legitimise the processing of sensitive data, the prohibition of processing sensitive data does not apply when a) data subjects have given their explicit consent; b) the data have manifestly been made public by the data subject; c) processing is necessary for the establishment, exercise or defence of a right in law; or d) processing is necessary to comply with an obligation of international public law.

[59] C. Cuijpers (2003), 'Het College Bescherming Persoonsgegevens', In: C. Cuijpers et al (eds), *Privacy concerns. Het delen van persoonsgegevens bij fusies, overnames en binnen concerns*, NVvIR, Elsevier, p. 89.

[63]. There is, however, one provision that provides for the approval of processing sensitive data by the CBP. Article 23, para. 1, sub e stipulates that processing of sensitive data can be legitimate if this is necessary with a view to an important public interest, where appropriate guarantees have been put in place to protect individual privacy, and when the CBP has granted an exemption. In granting such an exemption, the CBP can impose rules and restrictions.

[64]. The Personal Data Protection Act does have an obligation to *notify* the DPA (articles 27-30). The notification should contain the name and address of the data controller, the purpose of the processing, a description of the category or categories of data subjects and the data or categories of data relating to them, a description of the recipients or categories of recipients to whom the data might be disclosed, the proposed transfer of data to third countries, and a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing. The DPA and the Data Protection Officer (DPO) are obliged to keep a register of notifications. However, the most common and well known types of processing of personal data are exempted from this notification obligation, as formulated in the Exemption Decree (*Vrijstellingsbesluit Wbp*). The CBP website has an automated procedure that can be used by everyone to determine whether a data processing operation is exempted from notification.[60]

[65]. The DPA Annual Report 2007 provides empirical data with regard to compliance with the notification duty. From 2005 till 2007 the number of notifications received by the CBP increased from 27,999 to 32,349.[61] In 2007 alone 3,975 notifications were submitted to the CBP. The report does not provide precise information on compliance with the obligation to notify, but it does contain data on the frequency of sanctions imposed by the DPA. This concerns administrative fines, penalties imposed on a daily basis in case of non-compliance (*dwangsom*), and the compulsory enforcement actions (*bestuursdwang*). The report indicates that in 2007, no administrative fines and enforcement actions were imposed by the CBP, in contrast to 2006 when the CBP imposed three administrative fines and two enforcement actions. In 2007 the penalty imposed on a daily basis in case of non-compliance was imposed 39 times by the CBP.

[66]. In 2005, the Administrative Jurisdiction Division of the Council of State annulled a fine of € 15,000 by the DPA that was related to 11

[60] See http://www.cbpweb.nl/HvB_website_1.0/i1.htm, last consulted 07.02.2009 (in Dutch).
[61] The data mentioned in this paragraph are derived from the CBP's Annual Report 2007, p. 50, online at https://groupwork.uvt.nl/bscw/bscw.cgi/d2197763/Jaarverslag%20Cbp%202007.pdf, last consulted 07.02.2009.

processing operations that had not been notified.[62] The processing operations had already been started before the Dutch DPA came into force and therefore the Council of State concluded that the CBP was not qualified to impose a fine.

[67]. With respect to the *appointment of data protection officers*, article 63 of the Personal Data Protection Act stipulates the requirements that have to be met when appointing a data protection officer (DPO). Paragraph 1 of this article states that only natural persons with adequate knowledge for performing their duties and who can be regarded as sufficiently reliable can be employed as a DPO. The DPO has to be a natural person, therefore a legal entity, a committee, or the works council are not eligible for a DPO position. Second, with respect to the requirement of possessing adequate knowledge, the DPO needs to have knowledge about the organisation, the data processing occurring within the organisation, the interests involved, and ultimately, sufficient knowledge of privacy rules and regulations. Third, the requirement that the DPO has to be sufficiently reliable is reflected in the duty of confidentiality that has been incorporated in paragraph 4 of article 63. Moreover, this requirement is further supported by article 63, para. 2, which stipulates the independence of the DPO when performing his duties. Finally, article 63, para. 3 indicates that the DPO can only take up his duties after he has been registered with the CBP. Pursuant to the same paragraph, the CBP has the statutory task of keeping a public register of all registered DPOs. From 2005 to 2007, the number of DPOs increased from 183 to 240.[63]

[68]. Apart from the Personal Data Protection Act, there are also regulations regarding DPOs in article 34 of the Police Data Act. This DPO is appointed by the controller of the police data. His job is to monitor, on behalf of the controller, that the processing of police data is taking place in accordance with the Police Data Act and to give advice to the controller. He also has the duty to draw up protocols for the registration and dissemination of police data, and to draft an annual report with his findings. The controller must notify the police DPO with the CBP.

[69]. No evidence is available about the compliance in practice with the requirements for DPOs. The website of the Dutch Society of Data Protection Officers (*NGFG*) refers to the official requirements mentioned in the previous paragraphs, and does not contain other

[62] Afdeling Bestuursrechtspraak van de Raad van State, 21 September 2005, 200504372/1, LJN AU2998.

[63] See College Bescherming Persoonsgegevens, Jaarverslag 2007, p. 50, online at https://groupwork.uvt.nl/bscw/bscw.cgi/d2197763/Jaarverslag%20Cbp%202007.pdf, last consulted 07.02.2009.

guidelines or practicable instruments with respect to requirements for a DPO.[64]

[70]. Little evidence is available of the general compliance with the Dutch DPA or other data protection rules in practice. The second stage of the evaluation of the DPA (see above, para. [29]) provides some data about compliance; we refer to the report itself for details. The report's main conclusion are that the DPA's goals are not yet 'fully realised' in practice, and that the legal development, in the sense of sectoral standards and case-law, which calls for specific knowledge (sector, technology), has not yet materialised widely in practice.[65] In other words, the open norms are difficult for stakeholders to apply on the workfloor, and considerable work remains to be done to translate these open norms into workable, sector-specific and context-specific rules and practices. This does not necessarily imply, however, that data protection principles are not complied with. The findings from 1995 of an earlier social-scientific evaluation of the DPA's predecessor, the Data Registries Act (*Wet persoonsregistraties* (*WPR*)) found significant gaps in compliance with the details and letter of the law, but overall reasonably adequate compliance with the spirit of the law. Although the Data Registries Act itself was little known on the workfloor in daily practice, the persons responsible for maintaining data registries were often careful and conscientious in their handling of personal data, and they often intuitively complied with general data protection principles.[66]

4. Sanctions, Compensation and Legal Consequences

[71]. In the Netherlands, three types of sanctions can be applied in case of an infringement of data protection law. These are administrative enforcement actions (*bestuursdwang*), administrative fines (*bestuurlijke boete*), and penal sanctions (*strafrechtelijke sancties*).[67]

[64] See http://www.ngfg.nl, last consulted 07.02.2009.
[65] H.B. Winter et al. (2008), *Wat niet weet wat niet deert*, WODC 2008, http://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bescherming-persoonsgegevens-wbp-2e-fase.aspx#, last consulted 10.03.2009, p. 11.
[66] J.E.J. Prins et al. (1995), *In het licht van de Wet persoonsregistraties: zon, maan of ster? Verslag van een sociaal-wetenschappelijke evaluatie van de WPR*, Alphen a/d Rijn: Samsom, ITeR series Vol. 1.
[67] This section is largely based on: T. Hooghiemstra en S. Nouwt (2007), *Tekst en Toelichting Wet Bescherming Persoonsgegevens*, Den Haag: SDU, pp. 205-212.

A non-official sanction which can be applied in practice is negative publicity.[68]

[72]. The sanction of administrative enforcement action means that an order is given to terminate the situation that conflicts with data protection regulations, ensuring conformity with the law. If the accused does not fulfil his obligations within a certain period, determined in the written order, the CBP can take care of the obligations itself. Thus, the accused person or organisation first has the opportunity to solve the problem himself. In combination with the administrative enforcement action, the CBP can impose a penalty for each day the accused remains in default (*last onder dwangsom*). Administrative enforcement sanctions can be imposed in all cases where personal data are processed without conforming to the legal obligations from the Dutch DPA (art. 65). This implies mainly intentional practices. However, negligence in the sense of not notifying data subjects about the processing of their personal data also counts as a legal ground for administrative enforcement sanctions and penalties.

[73]. Administrative fines can be imposed with a maximum of € 4,500. The CBP is allowed to impose a fine in cases where there has been no notification or an incomplete notification of the CBP that personal data are being processed (art. 66). The fine is not imposed if the controller who can be held responsible for the violation can plausibly argue that he cannot be reproached for the violation.

[74]. Penal sanctions can be imposed for the same facts as for which an administrative fine can be imposed. Duplication of both sanctions is prevented by providing that no penal sanction can be given for a fact for which an administrative fine has already been imposed (art. 75 para. 5). Conversely, the provisions concerning the administrative fines stipulate that the right to impose an administrative fine ends from the moment that criminal proceedings for the same fact are started (art. 66 para. 5). When a controller acts in breach of the law, the penal sanction can be a fine with a maximum of € 2,250; intent or criminal negligence are not required (art. 75 para. 1). If the breach of law was however intentional, a maximum penal sanction can be imposed of a fine of € 4,500 or six months' imprisonment (art. 75 para. 2). In general, it appears that intent can be of influence on the level of a fine or other sanction. Depending on the impact of a breach of data protection legislation, the CBP can generate publicity for a specific case. Negative publicity can also be seen as a sanction towards a company that does not conform to the law.

[68] C. Cuijpers (2003), 'Het College Bescherming Persoonsgegevens', In: C. Cuijpers et al (eds), *Privacy concerns. Het delen van persoonsgegevens bij fusies, overnames en binnen concerns*, NVvIR, Elsevier, pp. 87-106.

[75]. The enforcement of data protection legislation largely depends on personal initiatives. There is an option that the public prosecutor will start criminal proceedings against a controller. However, these cases are extremely rare. Most cases have to be started by individuals who have been the victim of a breach of data protection legislation. In these cases, there will be civil proceedings. This implies that the party who loses the case has to bear the costs of the litigation, including court fees. The party starting the procedure has to pay a court fee to start a case. However, these costs become part of the entire costs of the procedure. The CBP and NGOs do not usually directly assist data subjects in a court case. The CBP has, however, declared that it aims to reduce its advisory task towards citizens and companies, and to expand its task of enforcement. Whether this means that the CBP will become more active in assisting in court cases remains to be seen, but at least there is the intent to have a more pro-active role when it comes to the enforcement of data protection legislation.[69]

[76]. In the context of employment, there are some specific safeguards to protect personal data collected and processed. Obviously, the general rules and provisions from the Dutch DPA apply. In addition, the Works Council Act (*Wet op de ondernemingsraden* (*Wor*)) includes some relevant provisions. Article 27 of this Act lists the cases where the board of a company needs the consent of the Works Council. With regard to data protection, articles 27 sub k and 27 sub l are applicable. Sub k states that consent of the Works Council is required in case of the establishment, amendment, or termination of a provision regarding the processing as well as the protection of personal data of the persons employed in the company. Article 27 sub l requires consent of the Works Council in case of the establishment, amendment, or termination of a rule concerning provisions aimed at or suitable for monitoring or checking of presence, behaviour, or performance of the employees. In case a decision is taken that conflicts with these rules, i.e. if the Works Council is not consulted or has not approved the decision beforehand, the decision is void if the Works Council hands over a written request for voidance to the employer. This means that Works Councils have an important role to play in monitoring the compliance with data protection legislation. It should, however, be noted that the establishment of a Works Council is only mandatory (and possible) for companies with at least 50 employees on a regular basis. Thus, for smaller companies this safeguard is not available.

[69] See CBP's memorandum, http://www.cbpweb.nl/documenten/med_20070808_beleidbudget.shtml?refer=true&theme=purple, last consulted 07.02.2009, mentioned in paragraph [54] above.

5. Rights Awareness

[77]. Not many data are available on people's awareness of data protection rights and obligations. The first stage evaluation of the DPA, however, indicated that many rights and obligations do not seem to be exercised due to lack of familiarity with the rules, both with the public and with small and medium enterprises and lower government organisations.[70]

[78]. Various surveys have investigated privacy perceptions and privacy awareness in the Netherlands.[71] In a 1989 survey, citizens seemed of the opinion that privacy is as important as good health care, a good environment, and fighting against unemployment and crime.[72] A 1999 survey was published by the Dutch Institute for Technology Assessment (*Rathenau Instituut*). The survey distinguished three groups of citizens: 1) citizens who think that information technology is necessary and who do not have any privacy problems with that (19%); 2) citizens who think that the increasing use of information technologies creates more privacy problems (35%); and 3) citizens who think that information technologies are a threat to privacy (47%).[73] A 2007 survey focusing on freedom and solidarity found that 51% of the respondents considered that the Dutch government sufficiently protects the fundamental right to privacy; 43% thought the government should protect their privacy better.[74]

[79]. A survey conducted within the European project PRIME analysed online activities of students and their trust in public and private institutions, their concerns with respect to personal data and privacy, and their knowledge and experience with privacy enhancing technologies (PETs). A comparison of respondents in the Netherlands, Belgium (Flanders), and the United Kingdom yielded the following conclusions:[75]

[70] G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009, p. 175.

[71] See also Sjaak Nouwt (2005), *Privacy voor doe-het-zelvers*, The Hague: Sdu, ITeR Series Vol. 73.

[72] Holvast, Jan, Henny van Dijk and Gerrit Jan Schep (1989), *Privacy Doorgelicht*, Den Haag: SWOKA.

[73] Smink, G.C.J., A.M. Hamstra and H.M.L. van Dijk (1999), *Privacybeleving van burgers in de informatiemaatschappij*, Den Haag: Rathenau Instituut, Werkdocument 68.

[74] Dieter Verhue, Harmen Binnema & Rogier van Kalmthout (2008), *Nationaal Vrijheidsonderzoek. Meting 2008. Opiniedeel*, April 2008, p. 36.

[75] I. Oomen & R. Leenes (2008), 'Privacy risk perceptions and privacy protection strategies', In S. Fischer-Hübner (Ed.), *Proceedings of IDMAN'07 – IFIP WG 11.6 working conference on Policies & Research in Identity Management*, Dordrecht: Springer, pp. 121-138.

- one fourth of the respondents will provide their true personal information and will not provide false answers;
- the respondents trust public institutions more than private organisations, with banks being an exception for they are trusted to the same extent as public institutions;
- British respondents are more concerned about possible consequences of abuse or misuse of personal data than Dutch and Belgian respondents;
- although respondents are also concerned about privacy issues, they are willing to provide personal information like their name, email address, gender, ethnic background, age, profession or occupation, educational level, religion, and marital status;
- personal information that is regarded as most privacy sensitive are credit card number and bank account details;
- the respondents feel that they do not have control over the way others collect their personal data and what others do with that data;
- more advanced privacy enhancing technologies are unknown to a large group of respondents;
- apart from country differences, also differences between men and women, differences between natives and non-natives, and differences with respect to field of study were found.

[80]. In January 2009, results were published of a survey executed by *Regioplan Beleidsonderzoek*, which was commissioned by the CBP. The report, *Nothing to hide but frightened nonetheless*, evaluates the attitude of Dutch citizens with regard to the collection and processing of their personal data.[76] The results are based on group talk sessions, a literature study, and a questionnaire answered by 2,016 citizens. It appeared that in general most citizens are rather willing to disclose their personal data. However, this does not mean that citizens are not aware of their privacy. Most citizens are aware, but their willingness to provide data can better be seen as a result of inevitability and a resigned attitude than in terms of trust that the data are used in a correct manner. In particular in the group talks, respondents showed themselves frightened when confronted with the risks of personal data processing. Nevertheless, this was no incentive to change their behaviour since that would require too much effort and the consequences would be too big. Control and transparency seemed important for the acceptance of data processing and citizens would be glad with overviews of their registered personal data on a regular basis. Furthermore, information on technological-societal

[76] J. Koffijberg et al. (2009), *Niets te verbergen en toch bang; Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving*, Amsterdam: Regioplan, publication number 1774.

developments is important and helps in the formation of privacy-aware attitudes. Finally, there is considerably more trust in a correct use and processing of personal data by the government than by private companies and institutions.

6. Analysis of Deficiencies

[81]. Several deficiencies regarding effective data protection and effective institutions have already been indicated above, in section 1.4, as emerging from the first stage of the evaluation of the Dutch DPA.

[82]. In addition to these, we can observe that some gaps emerge in legal certainty due to an unclear relation of data protection to other rules, for example, the Freedom of Information Act (*Wet openbaarheid van bestuur* (*Wob*)). Also, with some exceptions, the Dutch DPA does not apply to the processing of personal data for exclusively journalistic, artistic or literary purposes (art. 3 DPA). The scope of this provision is unclear. A broader interpretation of this exception has been suggested in order to bring websites outside the scope of the DPA more often, so that they will not be subject to unnecessary and unenforceable obligations. The Dutch supervisory authority has issued some criteria in this respect.[77]

[83]. Already in the evaluation of the predecessor of the Dutch Data Protection Act, it was emphasised that the legislation on data protection is too complicated to work with in practice.[78] In respect of the current DPA, these practical deficiencies are still relevant. The Brouwer Committee has recently concluded that the data protection legislation in the Netherlands has hardly been translated to the workfloor.[79] The second stage of evaluation of the DPA confirms that the translation of the DPA's open norms into workable, sector-specific and context-specific rules and practices still requires much work.[80] Besides the limited effect of the DPA in daily practice on the workfloor, mainly due to its complexity, also in court the effectiveness

[77] G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, last consulted 07.02.2009. p. 71; K. Versmissen, M. Schinkel & E. Kraai (2006), *Publicatie van persoonsgegevens op internet*, CBP, May 2006.

[78] J.E.J. Prins et al. (1995), *In het licht van de Wet persoonsregistraties: zon, maan of ster? Verslag van een sociaal-wetenschappelijke evaluatie van de WPR*, Alphen a/d Rijn: Samsom, ITeR series Vol. 1, p. 409.

[79] Commissie veiligheid en persoonlijke levenssfeer (2009), op.cit. n. 41, p. 39.

[80] H.B. Winter et al. (2008), *Wat niet weet wat niet deert*, WODC 2008, http://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bescherming-persoonsgegevens-wbp-2e-fase.aspx#, last consulted 10.03.2009.

of this legislation leaves a lot to be desired. Case law demonstrates not only difficulties in proving damage, especially in cases of immaterial damage, but also a lack of attaching proper consequences to acknowledged infringements of privacy.[81]

[84]. Several authors have also voiced concern over the future-proofness of the data protection system, in light of technological developments. It is questioned whether we can hold on to the current legislation regarding the processing of personal data when converging and ambient technologies become ingrained in our society.[82] As one scholar states: 'Signs that existing data protection legislation appears to be insufficient to deal with new technological developments must be taken seriously; normative and technological discrepancies between practice and Wbp (DPA) should be taken into account.'[83] Another scholar – one of the co-authors of this country report – has argued that the 'edifice of data-protection principles and data-protection laws [is based on assumptions that are] outdated and doomed to fail in the current information society'. In his view, the focus of data protection should be radically shifted: instead of focusing on data minimisation in the early, enabling stages of data processing, it should concentrate on correct data use in the later, usage stage of data processing.[84]

[85]. Altogether, many deficiencies, for example those relating to complexity and vagueness of the DPA, to a large extent relate back to Directive 95/46/EC. Solutions in this respect therefore are best to be found at the EU level. Awareness-raising and training data subjects and data controllers seems very important. However, practice and research demonstrate that even when they are informed of privacy concerns and privacy risks, citizens are inclined to easily provide their personal data in exchange for some kind of advantage, even as trivial as a ballpoint. In that light, it seems wise not to focus too much on data minimisation obligations, but to strengthen supervision of data processing. Giving greater priority to sanctions in combination with stricter enforcement will probably contribute more to improving

[81] C.M.K.C. Cuijpers (2007), 'Employer and Employee Power Dynamics.The division of power between employer and employee in case of Internet and e-mail monitoring and positioning of employees', 25 *The John Marshall Journal of Computer & Information Law* (1).

[82] Anton Vedder, 'Huidige bescherming privacy loopt ver achter', *Trouw* 28 October 2007; Jeroen Terstegge (2006), *RFID - A Future Policy Perspective*, http://www.rfidconsultation.eu/docs/ficheiros/terstegge.pdf, last consulted 07.02.2009; M. Hildebrandt & B.J. Koops (eds.) (2007), *D7.9: A Vision of Ambient Law*, FIDIS Deliverable, October 2007, http://www.fidis.net/resources/deliverables/, last consulted 07.02.2009.

[83] P. de Hert (2009), *Citizens' data and technology. An optimistic perspective*, Den Haag, CBP, p. 37.

[84] Bert-Jaap Koops (2008), 'Some Reflections on Profiling, Power Shifts and Protection Paradigms', in: Hildebrandt & Gutwirth (eds.), *Profiling the European Citizen. Cross-disciplinary perspectives*, Springer, pp. 326-337.

privacy and data protection.[85] To achieve this, a higher budget for the supervisory authority seems necessary. Also, improving understanding of the impact of privacy infringements, so that such infringements more often lead to exclusion of evidence in court or to awarding substantial damages, would probably likewise be beneficial for privacy and data protection. Finally, in view of the growing influence that technology has on our society, it seems appropriate to reconsider current legislation regarding privacy and data protection, not only in specific rules but also in its basic assumptions and systematic framework.

7. Good Practice

[86]. It is difficult to point out particularly good practices in data protection. Most of the literature restricts itself to outlining problems and deficiences rather than best practices. A few, fairly arbitrary, examples can be mentioned that we consider good practices. Mention can be made of the initiative of mutual recognition in Binding Corporate Rules (BCRs).[86] The Netherlands, together with several other EU Member States, joined the initiative to engage themselves to mutually recognise BCRs sent to them through the BCR coordination procedure. The essence of mutual recognition is that the DPAs commit themselves that once the Lead Authority circulates a consolidated draft with a positive opinion that it meets the required standard, other DPAs accept this opinion as a sufficient basis for providing their own permit or authorisation for the BCR, or for giving positive advice to the body that provides that authorisation. Simplifying and stimulating the use of BCRs in practice will help to overcome the difficulties in international data transfers within multinational companies.

[87]. Another example is the recent joint ruling by the CBP and the OPTA, the Dutch supervisory authority of post and electronic communications, regarding 'tell a friend' systems on websites.[87] OPTA and CBP agreed on a collaboration protocol on 30 June 2005 which is largely concerned with the division of labour when

[85] In this respect, Paul De Hert pleads for giving the supervisory authority more powers. P. de Hert (2009), *Citizens' data and technology. An optimistic perspective*, Den Haag, CBP, p. 39.

[86] See Article 29 Working Party, Press release, 2 October 2008, http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_02_10_08_en.pdf, last consulted 07.02.2009.

[87] The ruling states that "tell-a-friend" systems are allowed on websites subject to conditions. See OPTA and CBP (2008), Joint ruling, http://www.dutchdpa.nl/documenten/en_pb_2009_tellafriend_systems.shtml?refer=true, last consulted 07.02.2009.

addressing spam and other matters pertaining to privacy under the Telecommunications Act. Rather than strictly dividing tasks, the supervisory authorities in this ruling bundled forces, which can be considered a promising development. Cooperation between supervisory bodies will contribute to consistent interpretation of data protection legislation across various sectors in Dutch society and will thus help to overcome obscurities in practice.

8. Miscellaneous

[88]. In January 2009, the Brouwer Committee (*Commissie-Brouwer*), established by the government to advise on the balance between security and privacy, published its report.[88] This report aims at giving some principles and guidelines to protect security as well as privacy in practice. Usually, these two are seen as opposites that cannot be combined. However, the commission gives a number of principles to facilitate this combination. The 6 principles are:

- Transparency, unless…
  - In principle, citizens must know who does what with their personal data. Actively providing information on rights such as inspection, correction, and objection are key and contribute to the accuracy of data.
- Select before you collect
  - This principle is related to data minimisation and aims to implement the open wording of Article 8 (e) and (f) of the Dutch Data Protection Act.
- If necessary for security, you must share
  - If risk assessment reveals that the security of individuals is actually threatened, and the sharing of information may eliminate that risk, personal data must be shared. The commission proposes a similar approach when professional duties of confidentiality apply, and in that respect suggests embedding the principle of sharing when necessary for security more firmly in Article 9 of the Dutch Data Protection Act.
- Ensure integrity of data and action by users
  - Appropriate expertise is needed in the design of the systems.
- Ensure information and facilitation
  - Standard codes and protocols are essential. Development of good and best practices and simulations can

[88] Commissie-Brouwer (2009), *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer* [Do it simply – simply do it, to protect security and privacy], January 2009, http://www.minbzk.nl/116513/rapport-'gewoon-doen, last consulted 07.02.2009.

contribute to achieve the embedding of privacy interests in the work of professionals working in relation to security interests.

- Ensure compliance and internal supervision
  - Each institution or company that processes personal data should appoint an official with the authority necessary to enforce compliance.

[89]. While nationally and locally there is a focus on prevention, new collaborations are established between municipalities, police, the public prosecutor, and parties that were previously not involved in security regulation. An effect is the increased connection of databases and the indication of persons by means of profiling and data mining techniques. A related implication is that the information becomes disconnected from the source context. In the end, there can be 'images' of individuals that do not conform to reality anymore, which is indicated as the risk of the 'immutable me'.

[90]. Another point of attention is that more and more institutions are required to collect and process personal data. They often lack, however, the knowledge needed for safe and accurate data processing. This can put the privacy of individuals under tension. At an international level, the attention for security measures has not remained well-balanced with the protection of privacy. In the instances where there was attention for privacy, this was mainly to facilitate security measures. Internationally seen, there is no common vision on a balance between privacy and security.

[91]. In order to come to a balance and to make weighing easier, the commission is of the opinion that a framework for responsibly dealing with personal data is necessary. In this framework, the red line should be 'keep it simple, facilitate, expect the balance to be predominant, and work on a robust supervision and enforcement'.

Annexes

Annex 1 – Tables and Statistics

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority	2961	3919	4615	5014	5094	5898	5905	6147
Staff of data protection authority	51	52	54	61	65	62	72	72
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative	17	24	11	73	56	25	42	49
Number of data protection registrations	-	591	8454	21537	25565	27999	30078	32349

Number of data protection approval procedures ('voorafgaand onderzoek' / preliminary examination)	-	12	190	257	174	97	93	100
Number of complaints received by data protection authority, including requests for mediation	323	290	282	316	409	355	394	396
Number of complaints upheld by data protection authority	-	-	-	-	-	-	-	-
Follow up activities of data protection authority, once problems were established, disaggregated according to type of follow up activity: administrative fine (with regard to notification) / administrative order with conditional penalty / administrative enforcement	-	0/0/0	0/0/1	3/1/0	35/3/1	9/2/0	3/0/2	0/39/0
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority,	-	-	-	-	-	-	-	-

other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)								
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)	-	-	-	1.500-50.000	1500-15.000	1.500-15.000	1.500-3.000	5.000/week (50.000 maximum)

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	Lycos-Pessers
Decision date	25 November 2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Hoge Raad (*Supreme Court*), no. C04/234HR, *LJN*: AU4019
Key facts of the case (max. 500 chars)	Pessers, a Dutch lawyer and hobby stamp trader who offered stamps for sale on eBay, was accused of fraud by a Lycos customer on a website hosted by Lycos. Pessers demanded from Lycos (an internet service provider (ISP)) the personal data of this customer in order to take legal action.

Main reasoning/argumentation (max. 500 chars)	Lycos argued that it did not have to provide the subscriber data, inter alia, because this would be contrary to the Electronic Commerce Directive (2000/31/EC). That Directive provides that a so-called hosting provider (i.e. an ISP that hosts websites of its subscribers) is not liable for the information published on the website hosted by it, provided (a) that the provider does not have actual knowledge of illegal activity or information, or (b) that the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information. According to Lycos this implies that, being a hosting provider, it cannot be obliged to provide subscriber data to Pessers. They argue that the Directive provides for an exclusive arrangement regarding the hosting provider's liability: such a hosting provider can only be liable if he does have actual knowledge of the unlawful information and has refused to remove that information. As it was established that the information published on the website was not indisputably unlawful, Lycos argued that it was not liable and consequently could not be obliged to provide the subscriber data. In addition, Lycos argued that the provision of subscriber data would be contrary to the subscriber's freedom to spread information anonymously and that the subscriber's information should be protected. The Supreme Court did not agree with this. In the Court's opinion the announcement on the website did not have to be removed if the accusation was not indisputably unlawful. Nevertheless, that does not mean that the subscriber data does not have to be provided. If it is sufficiently plausible that information on a website could be unlawful, Lycos acts unlawfully towards Pessers by not providing the subscriber data on his request. In this respect, the Court also considered that the Directive requires that court actions allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Supreme Court's interpretation of the concept of 'unlawful' has led to some discussions in the Netherlands, as it means that ISPs should not only assess whether a web publication is indisputably unlawful, but also whether such a publication *could* be unlawful. That is, obviously, troublesome for ISPs, who in principle do not know and do not want to know the contents of the information distributed via their networks, servers and the like. However, the Supreme Court does introduce some restrictions. For instance, it asserts with some emphasis that: 'There is no general rule that anyone who has knowledge of particular information is obliged to provide this to the person who has a reasonable interest in the unknown information being communicated to him.' Furthermore, the Court remarks that its decision is tailored to the present case. Moreover, the Supreme Court also stipulated that "the interest of

	freedom of speech may not be passed over lightly, including in particular cases the interest of the website owner to utter its opinion anonymously."
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	It is expected that the decision will also have consequences, for instance, in the tracking and prosecution of internet users exchanging music, software and films via p2p-networks. In any case, the interest group of the copyright owners, the Stichting Brein (the Brein foundation is the joint anti-piracy program of authors, artists and producers of music, film and interactive software), which inter alia took legal action against KaZaA, is delighted by the decision. It is of the opinion that this will make it much easier to trace address data of Internet users who are suspected of illegal file-sharing. Moreover, the music business says that it will use it as a precedent to get details from Dutch ISPs to seek damages from people who illegally swap copyrighted music and over the Internet.
Proposal of key words for data base	ISP; third-party; unlawful; mandatory provision of personal data; third-party; Electronic Commerce Directive

Case title	Brein/UPC et al.
Decision date	12 July 2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	President van de Rechtbank (*Chairman of Regional Court*) Utrecht, *LJN*: AT9073
Key facts of the case (max. 500 chars)	Brein requested the Chairman of the Regional Court in a *kort geding* (a fast civil court procedure for urgent matters) to compel five internet service providers to disclose personal data of their customers. With this data Brein wanted to take legal action against customers who were offering illegal music on the internet through Kazaa. Without this data Brein would not be able to directly prohibit the offering of illegal music nor would it be able to

	claim damages from the customers. The internet service providers refused the request to provide the personal data of their customers and contended that only the criminal court is authorised to give an order to disclose the personal data.
Main reasoning/argumentation (max. 500 chars)	The Chairman of the Court ruled that the civil court is allowed to give orders to the internet service providers for the disclosure of personal data. However, this order cannot be given easily as it has to meet certain conditions. These conditions, stipulated in the Personal Data Protection Act, have been worked out by the Chairman of the Regional Court. In this specific case the Chairman of the Regional Court concluded that the refusal by the internet service providers was justified because Brein had called in the services of an American investigation bureau resulting in insufficient protection of personal data because the Dutch data protection standards were not met. Therefore the data processing by Brein was unlawful.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	This decision makes clear that, besides criminal courts, civil courts are also authorised to give orders for the disclosure of personal data by internet service providers. Moreover, it clarifies the conditions under which the civil court can give the order to disclose.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Court of Appeal upheld the decision of the Chairman of the Regional Court (Gerechtshof (*Court of Appeal*) Amsterdam, *LJN*: AY3854).
Proposal of key words for data base	ISPs; mandatory provision of personal data; civil order; criminal order

Case title	Dexia
Decision date	29 June 2007

Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Hoge Raad (*Supreme Court*), no. R06/045HR, *LJN*: AZ4663
Key facts of the case (max. 500 chars)	In December 2000 the respondent signed a securities-lease agreement with Dexia (the so-called 'WinstVerDriedub-belaar'). In 2002 the respondent made a request in writing for the sending of all of his personal data held by Dexia. Dexia reacted by sending a summary of the personal data held by its administration. The respondent was not satisfied by the provided information and on the basis of article 35 of Personal Data Protection Act requested a full overview of his personal data such as contracts, receipts and even transcripts of telephone conversations. Dexia refused the request.
Main reasoning/argumentation (max. 500 chars)	The central question of the dispute is whether Dexia has to allow inspection of and provide all of the personal data of the respondents in cassation, including the transcripts of telephone conversations, pursuant to Articles 35 and 46 section 1 of the Personal Data Protection Act. So far the lower judicial bodies have allowed most of the claims of the respondent in cassation. The Supreme Court ruled that the responsible party (i.e. Dexia) in the sense of the Personal Data Protection Act must provide full specific information to the data subject (i.e. respondent) involved, in order to enable such party to take note of its personal data and the manner in which they are processed. When requesting these data, the data subject only has to refer to Article 35 Personal Data Protection Act, and does not have to specify the grounds. The data subject is entitled to expect that the subsequently provided information will be transparent and complete. Furthermore, in order to comply with the obligations under Article 35 section 2 Personal Data Protection Act, the responsible party cannot suffice with the provision of general information, but has to provide all relevant information of the data subject. Depending on the circumstances of the case, the responsible party can meet this obligation by providing transcripts, copies or extracts. The interests of third parties can be taken into account in a proportional manner. The responsible party may only refuse the request to provide the copies and transcripts of telephone conversations, when it makes it sufficiently plausible that by the provision such administrative burden is so disproportionate, that

	its rights and freedom are infringed, or threaten to be infringed.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The decision gives a broader interpretation and application than earlier cases to article 35 of the Personal Data Protection Act which holds the right of the data subject to request personal data relating to him. A concise overview or summary provided by the responsible party may not be sufficient because according to this decision the data subject has the right to be provided with full disclosure of his personal data.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The novelty of this decision lies in the fact that it approves the requesting of transcripts of telephone conversations on the basis of article 35 of the Personal Data Protection Act.
Proposal of key words for data base	Article 35 Personal Data Protection Act; broad interpretation and application; telephone transcripts; complete disclosure

Case title	*Verwijsindex Antillianen*
Decision date	3 September 2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Afdeling Rechtspraak Raad van State (*Judicial Division of the Council of State*), no. 200706325/1, *LJN*: BE9698
Key facts of the case (max. 500 chars)	To do something about the disproportionate crime rate among youths of Antillean origin the former Dutch minister for Integration Rita Verdonk started a database which stored personal data of problematic Antillean youth, the so-called Reference Index Antilleans (*Verwijsindex Antillianen* (*VIA*)). The main rationale for setting up the database

	was that problematic Antillean youth are very mobile and are not always registered in a municipal register. Thus by setting up such database the government hopes to integrate and enhance the cooperative and monitoring activities between institutions dealing with this high-risk group in order to prevent crime and, in the end, to help overturn their disadvantageous position. Since the database concerns the processing of special personal data (i.e. ethnic origin Antillean) the Data Protection Authority provided an exemption for two years. The Dutch Caribbean Consultative Body (OCaN), which represents the Antilleans in the Netherlands, opposed the usage of the database arguing that the database is discriminatory and violates privacy. In 2007 the Regional Court ruled in favour of the OCaN indicating that the database is in breach of the Personal Data Protection Act. Several governmental bodies and the Data Protection Authority appealed against the decision and brought the case before the highest administrative court.
Main reasoning/argumentation (max. 500 chars)	The Judicial Division of the Council of State argued that the minister has made a convincing case that there are serious problems with the group of Antillean youth up to the age of 25 - more serious than amongst similar groups of different origin, therefore the usage of the database is justified. Furthermore, the court was of the opinion that the distinction in the case holds a 'legitimate aim' and processing data is 'suitable' for achieving that aim. Finally, the court concluded that granting the exemption is not in breach with the prohibition of discrimination laid down in the Dutch constitution and several international treaties.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The separate databank for high-risk youths from the Antilles may be terminated. The Dutch cabinet is now (December 2008) considering the inclusion of these youths in an alarming system for all youths in the Netherlands who risk becoming systematically involved in crime. It is not clear yet whether the ethnicity of high-risk youths will also be included in this other system. The cabinet has not taken a final decision yet on a common system for all high-risk youths.

Proposal of key words for data base	Personal Data Protection Act; Exemption; Ethnicity;

Case title	Mariëndijk
Decision date	29 September 2004
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Strafrechtkamer Rechtbank (*Criminal Division of the Regional Court*) 's-Gravenhage, no. 09.755.033/03, *LJN*: AR2973
Key facts of the case (max. 500 chars)	Under false pretence and unlawful and improper practices the business information agency Mariëndijk was specialised in tracing personal data about persons –mainly debtors- for their customers, usually creditors such as banks, insurance companies and law firms. Most of the information requested by their customers, such as information about the income, criminal record or outstanding debts of a certain person, could only be obtained by approval of the person concerned. Nevertheless, the agency managed to extract this sort of privacy-sensitive information from non-public sources by improper and unlawful practices. One director of the agency was indicted and brought to the criminal division of the regional court.
Main reasoning/argumentation (max. 500 chars)	The suspect, as a director of the business information agency, had given orders to other persons for a financial consideration to acquire mostly confidential information from non-public sources. The information from these sources was obtained by improper means, by agency's employees' and third parties who approached institutions telephonically and used false names and presented themselves as colleagues of similar institutions.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	None.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The suspect was convicted for fraud and it was proved that the suspect had violated article 27 section 1 of the Personal Data Protection Act which encompasses the obligation to notify the Data Protection Authority in case personal data are being processed.
Proposal of key words for data base	Fraud; prosecution; article 27 Personal Data Protection Act