DUTCH DPA

PUBLICATION OF PERSONAL DATA

ON THE INTERNET

DECEMBER 2007

CONTENTS

Dutch DPA Guidelines

PUBLICATION OF PERSONAL DATA ON THE INTERNET

December 2007

INTRODUCTION

Respect for privacy is viewed as an essential provision for a dignified existence and as one of the foundations of our legal system. Everybody has the right to protection against the uncontrolled collection, processing and distribution of their personal data.

Personal data are published on the Internet in many different ways. Due to its nature, the Internet makes it easy to publish personal data, for example, via a website, in a discussion forum, or in an online journal. People can publish data about themselves, or about others. Publications on the Internet are generally accessible worldwide, 24 hours per day, to a potentially extensive and highly varied public. The consequences could be huge for people whose personal data are placed on the Internet, for example, if they relate to unproven suspicions or intimate details relating to their personal life. Even if the data are correct, publication on the Internet can cause an incomplete representation of a person, which could lead to that person being judged negatively.

For that reason, the law imposes restrictions upon the permissibility of publishing personal data on the Internet.

The principal rule of the Wet bescherming persoonsgegevens (hereinafter referred to as: Wbp) [Dutch Data Protection Act] is that each person who publishes personal data is personally responsible for compliance with the Act. Individuals, companies, organisations and institutions that have the intention of publishing data relating to persons on the Internet, must therefore assess, prior to publication, whether publication is in fact permitted, and if it is permitted, with which provisions they must comply.

The Dutch Data Protection Authority (hereinafter referred to as: Dutch DPA) [College bescherming persoonsgegevens (CBP)] wishes to make this easier to assess by providing these guidelines. This is in the interest of those who publish on the Internet and in the interest of the people in respect of whom data are (or could potentially be) published.

These guidelines deal with the basic rules that controllers should follow when assessing the publication of personal data on the Internet, subject to the applicable privacy legislation and case law[1)].
The guidelines focus primarily on the World Wide Web.

Publications may be unlawful for reasons other than the protection of privacy, for example, because they contravene the Auteurswet [Copyright Act]. The handles in these guidelines are limited to the permissibility of the publication under the applicable privacy legislation. These guidelines therefore do not discuss the lawfulness of publication on the basis of other legislation.

The guidelines cover many of the most important regulations in relation to the protection of personal data, but do not comprise an exhaustive description of all existing statutory provisions and case law. The examples that have been included in these guidelines serve only as an illustration of the way in which the Dutch DPA implements a specific provision of the Wbp when assessing a publication. Forms of publication that have not been included in these guidelines as an example may nevertheless contravene the Wbp.

Other provisions than the provisions of the Wbp that are discussed in these guidelines may play a role when assessing a publication that is comparable to an example. Even in the event that a specific (type of) publication is very similar to one of the examples, the publisher must be prepared for the fact that the final assessment can only be made by taking into account all of the circumstances relating to the individual case and that the assessment may therefore have a different result.

These guidelines do not anticipate court judgments. In addition to legislative changes, technological developments and practical experiences, court judgments may give cause for supplementation or revision.

These guidelines will come into force with effect from 11 December 2007, which is the date of their publication in the Government Gazette.

1) The legal framework primarily comprises the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act] (Act of 6 July 2000, Bulletin of Acts, Orders and Decrees 302), the case law of the European Court of Human Rights (ECHR), the European Court of Justice (ECJ) and relevant interpretations of Article 29 Working Party, the co-operation of data protection authorities in the European Union (EU). Where relevant, the general case law of the Netherlands will be considered, in addition to the judgments of the Dutch DPA itself.

FLOW CHART

Are you a natural person, company or institution that bears responsibility for a publication on the Internet? (see I.2, page 7)

NO ➤ These guidelines do not apply to you. In the chapter entitled 'Data subjects' rights', you can read what your rights are if your personal data are published on the Internet against your wishes.

YES ⮟

Does the publication contain data pertaining to (living) natural persons? (see I.3 to I.6 inclusive, page 9)

NO ➤ The Wbp applies exclusively to data that can be traced back to (living) natural persons. These guidelines do not apply to your publication.

YES ⮟

Do the data relate to criminal data, a person's religion, personal beliefs, race, political persuasions, health, sexual orientation, or membership of a trade union? (See I.8, page 14)

YES ➤ Publication on the Internet is NOT permitted, unless the person to whom the data relate has given his or her express consent, or has clearly publicised the information in question him or herself. (See I.8.1.1 and I.8.1.2, page 15)

NO ⮟

Do the data include identification numbers, such as the person's Citizens Service Number? (See I.8.3, page 16)

YES ➤ Publication on the Internet of identification numbers is NOT permitted. (See I.8.3, page 16)

NO ⮟

Is this a publication to which access is effectively restricted to the person's household, family members and/or acquaintances, for example, by means of a password? (See I.7.1, page 12)

YES ➤ The publication falls under the exemption for personal/household use; the Wbp does not apply.

NO ⮟

Is this a publication for exclusively journalistic, artistic or literary purposes? (See I.7.2 and IV, pages 13 and 42)

YES ➤ The Wbp applies in part.
The following apply:
– definitions (I.2 to I.6 inclusive, page 7)
– due care and attention (page 7)
– purpose and compatibility (II.2 and II.3, page 19)
– consent or necessity (II.4, page 21)
– quality (II.7, page 30)
– security (II.8, page 32)

NO ⮟

Do you have the consent of the data subject or can you demonstrate that it is necessary to publish personal data on the Internet? (See II.4, page 21)

NO ➤ You are not permitted to publish personal data on the Internet without having grounds rendering the publication legitimate, as expressed in Article 8 of the Wbp.

YES ⮟

If your publication is based upon the consent of the data subject, can you remove personal data if requested to do so?

NO ➤ Each person is entitled at all times to withdraw his or her consent. Once consent has been withdrawn, the publication will no longer be justified; the personal data must be removed. (See II.4.1.1, page 22)

YES ⮟

Check whether you fulfil your obligations in relation to:
– purpose and compatibility (II.2 and II.3, page 19)
– the obligation to provide information (II.5, page 25)
– the notification obligation (II.6, page 29)
– quality (II.7, page 30)
– security (II.8, page 32)
– data subjects' rights (III, page 38)
– transfer to countries outside of the EU (V, page 48)

BASIC PRINCIPLES IN RELATION TO THE PROTECTION OF PERSONAL DATA ON THE INTERNET

1 Introduction

Personal data on the Internet must be treated with the same care as they are offline. The Act applies to 'fully or partly automated processing of personal data'[2], and therefore to all publications of personal data on the Internet.[3] Each entity that publishes personal data on the Internet, regardless of whether this is a private individual, a company, an institution or an administrative body, must fulfil the obligations imposed by the Act. These are: to act with due care and attention, transparency, consistency with the purpose, justification, quality and proportionality, rights to information, security and restriction of transfer to countries outside of the EU.

Article 1 of the Wbp contains definitions of the terms used in the Act. Not all of the terms are equally relevant for assessing publications on the Internet. The most important of these terms are included below. The following text also briefly explains three important exemptions from the applicability of the Wbp: the processing of personal data for personal/household use; the processing of data for exclusively journalistic, artistic or literary purposes, and the use of data for historical, statistical and scientific purposes.

2 Upon whom does the law impose obligations? The controller

In these guidelines the term 'controller' is understood to refer to the person that under the Wbp, bears responsibility for the content of an Internet publication. In accordance with the Act, this is the natural person, legal entity, administrative body or any other party that, either alone or in conjunction with others, determines the purpose and the means for processing personal data.
The controller may be the owner of a website, the creator of a personal profile, but also the owner/administrator of a discussion forum. In a discussion forum, or in an article in which visitors are given the opportunity to respond, readers may submit contributions that contain personal data. In principle, each individual who contributes is personally responsible for incorporating this personal data, however, the general responsibility for exercising due care when processing data lies with the owner of the forum, because after all, it is that person who determines the purpose and the means. The owner of the website or forum, the person who has formal-legal control over the processing, provides visitors with the opportunity to publish data and is therefore obliged to ensure that personal data are treated with due care and attention.[4]

WEBSITE IN THE UNITED STATES

A controller situated in the Netherlands can opt to employ technical means outside of the Netherlands for a publication, for example, by making use of web hosting[5] in the United States. Although the website is not located within the territory of the Netherlands, the Wbp applies nevertheless. The Wbp applies to all controllers who are resident within the Netherlands.

2) The Act also applies to non-automated processing, such as paper files, but only in the event that the data have been or are incorporated in a file, i.e. a structured whole of personal data that is accessible in accordance with specific criteria and related to various persons.
3) Explanatory Memorandum [Memorie van Toelichting] to the Wbp, Parliamentary Documents II, 28 509, 3, page 71: 'Once information has been recorded in electronic form, this is considered in all cases to have undergone automated processing of data. After all, an automated system enables searching for digital data. (...) The fact that due to automation, digitally recorded sound and image information can be compared at a speed and on a level of detail that are incomparable to carrying this out manually, is a justification for a stringent legal regime.'
4) 'Any person who has recorded and uses personal data, for example by offering the data as reference, even if the data are anonymous and have been provided by a third party via the Internet, is accountable for compliance with this legislative bill and cannot plead the excuse that he or she had no involvement in the communication. The data is considered to have been processed as soon as it has been stored with a view to being used as a reference, for example in the form of a 'cache-service.' Explanatory Memorandum, page. 60.
5) Web hosting is hiring out disk space on an Internet server (usually for a fee) on which controllers can place Internet pages. Such servers may exist within the EU, but also outside of the EU. The web hosting company has no control over the content of the publication.

The owner of a discussion forum is an intermediary on the Internet. All actions on the Internet involve an intermediary. Other intermediaries include Internet access providers, parties providing web hosting services and search engines. The term 'controller' referred to in the Wbp is used in a broad context and therefore also applies to some intermediaries.

Access providers do not have any control over the transfer of personal data. They therefore cannot be classed as a controller, except in the case of information provided by the access provider on its own initiative and that has been edited by the provider itself, for example via a newsletter. This does not apply to the owner/administrator of a discussion forum, as this person has legal and actual control over the data on the forum, determines the aims of the forum in the first and last instance and is responsible for operating the forum.

In the case of the hosting of material, the creation of a hyperlink to personal data and the use of material on the Internet by search engines, account should be taken of the degree of control these services have over the processing of personal data. The question of whether an intermediary has control over the removal of the data is particularly important. The answer to this question is yes if an intermediary is able to delete information and is accustomed to doing this in certain cases where third parties have drawn his or her attention to instances of unlawful publication. This type of intermediary is responsible for processing personal data published by third parties (particularly with regard to keeping this data available, removing or blocking it) and, on this basis, is jointly responsible for this type of processing.

The term 'data processor' referred to in the Wbp does not apply to a service provider if the service provided to the controller does not explicitly relate to the processing of personal data. It shall therefore in principle not be possible to regard the intermediaries referred to as data processors.

THE DIFFERENCE BETWEEN RESPONSIBILITY AND LIABILITY

Under the terms of the Wbp, there is a difference between 'responsibility' and 'liability'. Some intermediaries are, subject to certain conditions, released from liability in respect of the unlawful actions of third parties. This involves services provided by an information society consisting of the provision of access, the temporary storage and hosting of material. These regulations arise from the Electronic Commerce Directive and can be found in Article 6:196c of the Burgerlijk Wetboek (BW) [Netherlands Civil Code]. The dividing line between a controller and a non-controller in the Wbp is not in line with the release of some intermediaries from liability. It is therefore possible for a service that, pursuant to Article 6:196c of the BW, must be regarded as a hosting service (section 4), to be a controller under the terms of the Wbp. In this case, the provider is not liable in respect of the unlawful processing of personal data by third parties. The provider must, however, delete the information or make it impossible to access such information as soon as he or she is aware or could reasonably be expected to be aware of any unlawful activity. In view of the nature of the regulations under the Wbp and the limited ability on the part of intermediaries to determine the lawfulness of the publication of personal data, this obligation to block or delete information shall only arise in the event of an obvious breach of the Wbp.

The above means that, in practice, intermediaries who are able to invoke a statutory release from liability can use the regulation with associated conditions in Article 6:196c of the Netherlands Civil Code as a guideline.

The term 'data subject' is understood to refer to the person whose personal data are being processed. On the Internet, the roles are frequently interchangeable; a person who maintains a personal weblog can be both the controller and the data subject.

3 What constitutes personal data?

The Wbp comprises a liberal definition of personal data. In Article 1, subsection a of the Wbp, an item of personal data is defined as 'any item of data relating to an identified or identifiable natural person'. The description has been literally adopted from Article 2 of the European Data Convention.[6)]
The European Privacy Directive 95/46/EC (hereinafter referred to as 'the Directive'), upon which the Wbp is based, provides a somewhat more extensive description.

Article 2, subsection a of the Directive provides the following definition of personal data:
Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Although the second section of the European definition, i.e. the explanation of specific elements that make a person identifiable, has not been adopted in the Wbp, the Explanatory Memorandum [Memorie van Toelichting] to the Wbp clarifies that the Wbp employs the same principle in respect of indirectly identifying personal data.

The first thing that is relevant to the term 'personal data' is whether the data comprises information relating to a person. In many cases, such as factual or appreciative data regarding characteristics, opinions or behaviours, this will ensue from the nature of the data. In other cases, attention will also have to be devoted to the context in which the data are recorded and used. In the event that the data partially determine the way in which the data subject is judged or treated in society, these data must be viewed as personal data. The (social) use of data therefore determines, in part, the answer to the question of whether an item of data is considered to be personal data.[7)]

The Article 29 Working Party of cooperating data protection authorities in the EU, elaborated upon the various sections of the definition of personal data in a recent opinion. This relates to the terms 'any information', 'relating to a natural person' and 'directly or indirectly identifiable'.

PROFILE SITES

Profile sites are particularly popular amongst young people. They use profiles to show who they are, who their friends are and how many friends they have. They write about what they do and what they like, as well as leaving personal messages on other peoples' profiles. The more information a person provides about him or herself, the better able he or she is to show that he or she is worth the effort. Many young people go to great lengths in terms of sharing information on publicly accessible profiles, for example posting stories about parties, drug use and sex.

The providers of profile sites are, together with the users, jointly responsible for the processing of personal data on the relevant website. The providers of these types of services are therefore required to observe the regulations under the Wbp. This means that they must provide users in advance with comprehensive information regarding the availability of profiles to other visitors to the site. They must take appropriate security measures, such as ensuring that the profiles have a standard level of protection with regard to search engines, as well as ensuring that only friends of the user have access. They must also offer the option to delete the profiles and information posted elsewhere on the site.

3.1 Any information

The Working Party emphasises that 'any information' includes both objective and subjective data, regardless of whether they are correct or proven. Consider, for example, opinions such as 'John is a reliable lender' or 'John is a good employee who deserves a promotion.'[8)]

3.2 Relating to a person

In order to determine whether an item of data relates to a person, the Working Party specifies that one of the following three elements must be present: a content element, a purpose element or a result element.

6) Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg 1981, Treaty Series 1988.
7) Explanatory Memorandum to the Wbp, Parliamentary Documents II, no. 25 892, no. 3, page 46.
8) Opinion 4/2007 on the concept of personal data of the Article 29 Working Party, adopted on 20 June 2007, page 6.

A content element means that the information relates to a person, regardless of the purpose of the controller or the result for that person, such as the results of a medical analysis relate to the patient, or such as the data in a customer file of a company relate to the customer.

The presence of a purpose element may also lead to data being considered as personal data. This is the case if the data are (likely) being used for the purpose of treating somebody in a particular way or to judge or influence his or her status or behaviour. This may be the case if a company maintains a database comprising an overview of all incoming and outgoing telephone calls. That database can be used to assess employees.

If a content or purpose element is not present, the data may nevertheless be personal data, if the use of this data will probably have an influence upon the rights and interests of a person, in the sense that this person will be treated in a different manner as a result. That may be the case if a taxi company monitors the locations of its taxis by means of GPS. Although the system is designed for processing data regarding the routes of vehicles, the data may also be used to assess the individual taxi drivers.[9)]

3.3 Directly or indirectly identifying

The most well-known directly identifying item of data is the combination of forename and surname. The most well-known indirectly identifying items of data include (e-mail) addresses, telephone numbers, car number plates and the combination of post code/house number.[10)] Other indirectly identifying data include data regarding a person's characteristics, beliefs or behaviours that distinguish that person from others, for instance, the director of a specifically named company.

IP-ADDRESS

Could an IP address, that is to say the Internet address used by a computer to communicate its identity on the Internet, be classified as an item of personal data? Yes. An IP address is an item of personal data, because a third party, the Internet service provider, can easily trace it back to a natural person, i.e. the Internet subscription customer. This is also the case with dynamic IP addresses processed in combination with date and time. It makes no difference whether or not a controller will be using the IP address to identify an individual. The mere fact that the controller or a third party has the option to do this is sufficient. The fact that, in some cases, the IP address identifies a legal entity, instead of a natural person, does not detract from the fact that, in the majority of cases, this is indeed personal data and that therefore the entire collection must be treated in accordance with the principles of the Wbp. In addition, it is important that decisions can be made regarding access to certain information on the basis of the IP address, without a service provider having any difficulty at all in associating personal data to an IP address. Consider, for example, distinctions being made between geographical origin when determining access to and the presentation of (sections of) websites[11)]. The registration and possible publication of IP addresses on the Internet of visitors to a website, or of participants in a discussion forum, therefore falls within the scope of the Wbp.

When deciding if an item of data would be considered as indirectly identifying personal data, it is important to examine whether the identity of the person can be determined, within reason, by means of the data and without disproportionate efforts. Whether identification actually takes place is not the decisive factor in this instance. This view stems from consideration 26 of the privacy directive: *Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.(…).* It therefore suffices for the purposes of making the decision, to examine whether the item of data can be traced back to a natural person, to such an extent that a third party can achieve this by reasonable means.

9) Opinion 4/2007, pages 9-12.

10) The Registratiekamer [predecessor of the Dutch DPA] and the Dutch DPA have issued decisions on telephone numbers (including: Registratiekamer, 8 July 1993, 93.1.002 and Dutch DPA, 28 May 2003, z2003-0480, on the blocking of numerical data, URL: http://www.cbpweb.nl/documenten/adv_z2003-0480.stm); on the registration of car number plates (including: Registratiekamer, 9 December 1996, 96-0140 process control through registration of number plates, URL: http://www.cbpweb.nl/downloads_uit/z1996-0140.pdf) and on postal codes and house numbers (including: Registratiekamer 21 June 1996, 95.O.043).

11) Opinion 4/2007, page 14: 'Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense.'

4 When is an item of data not an item of personal data?

Data relating to organisations, such as companies or foundations, are not considered to be personal data in the sense of the Wbp. The Act does however apply to companies if the data identifies a person, such as in the case of a one-man business, or if it relates to the individual directors of a company or foundation.

Equally, the Wbp does not apply to data relating to deceased persons. If, however, the data of a deceased person relate to a surviving relative (for example in the case of information relating to a hereditary disease) the Wbp may indeed apply.

GENEALOGICAL WEBSITES

An increasing number of sources are available on the Internet for those who are interested in researching their family tree, including both electronic archive material and research conducted by (amateur) genealogists. Since the Wbp does not apply to deceased persons, few objections can be made on the basis of the Wbp to the publication of a family tree on the Internet. Nevertheless, the Dutch DPA frequently receives queries and complaints regarding family trees on the Internet. Since genealogists understandably have a desire to include as much information as possible, many family trees include information relating to living persons, such as their date of birth. Some family trees even state the illness to which people have succumbed. Such information may relate to surviving relatives and therefore constitute personal data in the event that it relates to a hereditary disease that may affect the children. That may be so in the case of a mother who dies from haemophilia. Since this illness is related to a gene in the X-chromosome, she passes the illness on, in any case, to her sons. In this instance, the Wbp does indeed apply. Those who wish to publish a family tree on the Internet would therefore be wise to limit themselves initially to data relating to deceased persons, and only include data relating to living persons if they have received unequivocal consent to do so. The Wbp does not recognise the principle 'silence lends consent', when it comes to publishing personal data on the Internet. The publicist must have made reasonable efforts to contact the (living) family members and tell them – prior to the publication of their personal data on the Internet – what he or she wishes to publish about them and the purpose of the publication. In the event that a family member withholds his or her consent to such a record, publication of his or her data is not permitted. The publicist can include a reference in the family tree on the Internet, such as in the following example: 'This marriage resulted in the birth of three children, including...'

Data relating to properties are generally not personal data either. In marginal cases, the context in which the data will be used is important. Data relating to property, such as private residences, are considered to be personal data if the information can be used to judge the residents or owners and to draw conclusions from this, such as the amount of tax levied against the occupants.

PANORAMIC PHOTOS OF HOUSES

In 2001, the Registratiekamer (the predecessor of the Dutch DPA) conducted research into the use of geographical information.[12] A company made digital recordings of public areas with a 360 degree image. The images could be searched according to municipality, town, street and house number. Since the owners and residents of the properties in question could be identified without the need for a disproportionate amount of effort and furthermore, the digital images were used by municipalities to assess the value of properties, the Registratiekamer determined that the photos constituted personal data for which the producers and the customers were responsible according to the Wbp.

5 Anonymous or pseudonymous data

Anonymous data are not personal data in the event that the data subjects are not identifiable using reasonable means. The question of whether an item of data is in fact anonymous is specifically raised during the publication of statistical information on the Internet. Aggregated information may contain personal data if the number of data subjects is small and other information is available, for example, by means of search engines, enabling identification of individual persons.

Data are sometimes not considered to be personal data if they have been assigned pseudonyms, depending on the method of encryption used. However, the data must be treated as personal data, in so far as the controller, or a third party, can still use the data to identify natural persons, without the de-

12) Registratiekamer, 16 February 2001, z2000-1172, URL: http://www.cbpweb.nl/documenten/uit_z2000-1172.stm

ployment of disproportionate efforts.[13] This may be the case when pseudonyms are used for contributions to a discussion forum. Even in the event that just a single forum administrator knows the identity of the data subject, the pseudonym then becomes an identifying item of data and therefore constitutes an item of personal data in all instances in which the pseudonym is used. The use of pseudonyms can also lead to items of data becoming identifying in other ways. Many people use the same pseudonyms for all of their activities on the Internet. Data subjects' personal details may, as a result of search engines, unintentionally be linked to contributions that were intended to be anonymous.

6 Lifetime of the publication

Controllers of publications on the Internet must account for the consequences of the frequently long or undetermined lifetime of a publication. Due to technological developments, an item of data that does not appear to be personal data at the time of publication may nevertheless identify a person at a later stage. From that moment onwards, controllers can be subjected to legal action under the terms of the Wbp.[14] For that reason, it is important that controllers who do not wish to act in contravention of the Wbp, ensure that they apply a limited term, taking into account the risks, to the publication of data that do not appear to be personal data and also to take action immediately upon realising that the data can be used to identify persons.[15]

THE PUBLICATION OF MINUTES OF MEETINGS

An organisation decides to place the minutes of meetings on the Internet so that everyone within or outside of the organisation is able to see how the organisation functions. If the reports contain personal data, the controller must observe the regulations under the Wbp. If the public nature of the reports is not legitimised by the activities of the organisation or the employment relationship, the controller must in principle obtain consent from those involved. In particular, the controller must establish a limited term for the publication of the documents on the Internet. A term of two years would appear to be sufficient for the purpose of demonstrating how an organisation functions. The use of a web publication system that provides the option to automatically impose this term is a simple example of the use of Privacy Enhancing Technologies.

7 Exemptions from the applicability of the Wbp

There are three types of data usage in relation to which the Wbp does not apply or only partially applies. These are: processing for personal or household use, use of data for exclusively journalistic, artistic or literary purposes and use of data for historical, scientific or statistical purposes.

7.1 Personal or household use

The first exemption is the most absolute. The Wbp does not apply in any way to the processing of personal data exclusively for personal or household purposes. The objective of this is to prevent everyday actions of private individuals, such as keeping an address book, from falling within the scope of the Act.

The exemption for personal/household use provided for in the Wbp relates to use for 'a clearly predetermined group of people'.[16] The exemption also applies for use by family members or friends that do not form part of the immediate household, provided that access has been actively limited to a predefined group of family members, acquaintances or friends.

13) See Opinion 4/2007 for further examples, pages 18-21.
14) Parliamentary Documents II, 25892, no. 9, page 2. See also the Explanatory Memorandum, page 49: 'Therefore, those items of data which, in view of the current status of technology, may be perceived as anonymous, as they cannot be used to identify a natural person through the deployment of reasonable means, may, at a later date, become personal data due to technological developments, in view of the increased opportunities for traceability'
15) Opinion 4/2007, page 15: 'If the data are intended to be stored for one month, identification may not be anticipated to be possible during the "lifetime" of the information, and they should not be considered as personal data. However, if they are intended to be kept for 10 years, the controller should consider the possibility of identification that may occur also in the ninth year of their lifetime, and which may make them personal data at that moment. The system should be able to adapt to these developments as they happen, and to incorporate then the appropriate technical and organisational measures in due course.'
16) Explanatory Memorandum, page 70.

Those who wish, for example, to maintain a weblog on the Internet for their own family and wish to refer to the exemption for reasons of personal or household use, must take appropriate measures to actively limit access to this restricted circle. This can be achieved, for example, by applying an obligatory password, but also by blocking the pages that contain personal data from search engines. Chapter 2.8 of these Guidelines provides further information on security measures.

At the moment that the data are disclosed to an unknown number of people, however, which is the case when publications on the Internet are freely accessible, the Wbp applies in full.[17] Many personal publications that are intended for a restricted circle of interested parties therefore fall under the scope of the Wbp.

These may include a website to welcome a newborn baby, images of holiday activities or a weblog comprising a personal commentary on day-to-day events. If any interested party can view the publication and the personal data are not blocked against further processing by search engines, the Wbp applies in full.

7.2 For exclusively journalistic, artistic or literary purposes

The Wbp applies in part to data processing on the Internet exclusively for journalistic, artistic or literary purposes.[18] In that respect, the legislator sought a balance between the right to protection of personal data and the right to freedom of expression. Chapter 4 of these guidelines explains this balance and elaborates upon the issue of whether a publication on the Internet fulfils the criteria of 'exclusively journalistic, artistic or literary purposes'.

7.3 For historical, statistical or scientific purposes

Finally, there is a ground for exemption from the applicability of the Wbp[19] that enables personal data collected for another purpose to nevertheless be used for historical, statistical or scientific purposes.

Controllers who want to publish personal data on the Internet within the scope of scientific, historical or statistical research must take the necessary measures to ensure that the data are processed only for these specific purposes[20] These may be technical measures, such as blocking the publication with a password (see also Chapter II, section 8 on security), legal measures, such as recording the uses to which the data may be put in a contract, but also organisational measures, such as the setting up of a procedure to assess requests for access individually. This exemption will therefore, in practice, only apply to strictly guarded intranets.

The controller may also retain such data for longer than is strictly necessary for the original purpose, provided that effective security measures are once again taken against improper use.[21] Finally, in some cases, institutes or services for scientific research or statistics do not need to fulfil the obligation to provide information and the right of access.[22]

17) Explanatory Memorandum, page 69: 'When developing the Directive, the Council of Ministers and the European Commission made notes in relation to this, stating that this formulation may not give rise to the processing of personal data by a natural person, in cases in which these data are not disclosed to one or more persons, but to an unspecified number of persons, being exempted from the Directive.'

18) Consideration 17 of the Directive: 'Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9.'

19) When the Wbp was under discussion in the Lower Chamber, the Minister explicitly specified that this was not a general exemption, but rather, it was 'a sectoral specification of the requirement for consistency in the form of an irrefutable presumption of law'. Parliamentary Documents II, no. 25 892, no. 6, page 17.

20) Article 9, paragraph three of the Wbp: 'Further processing of the data for historical, statistical or scientific purposes is not viewed as incompatible if the controller has taken the necessary measures to ensure that further processing takes place exclusively for these specific purposes.'

21) Article 10, paragraph two of the Wbp: 'Personal data may be retained for a longer period than that which is specified in the first paragraph, provided that they are being retained for historical, statistical or scientific purposes, and in so far as the controller has made the necessary arrangements to ensure that the data in question are exclusively used for these specific purposes.'

22) Article 44 Wbp: 'In the event that data are processed by institutes or services for scientific research or statistics and the necessary arrangements have been made to ensure that the personal data can only be used for statistical and scientific purposes, the controller can omit the statement as referred to in Article 34 and can refuse to comply with a request as referred to in Article 35.'

PUBLICATION OF INTERNET STATISTICS

Many controllers maintain statistics about the use of their website, including IP addresses and search terms for example, for statistical purposes. Those who publish such statistics on the Internet cannot be certain of the purpose for which visitors to their website process these data. In order to provide an open insight into the use of the site, data regarding the number of visitors and the most frequently used search terms[23] can be published in an anonymous format. For internal use, however, the statistics may be made accessible to employees that require access in order to perform their duties.

The publication of an archive comprising personal data on the Internet, for example a collection of historical homepages, for historical, statistical or scientific purposes, is only permitted if the controller has taken the necessary measures to ensure that the data are exclusively used for that specific historical, statistical or scientific purpose. If an archive comprising personal data also contains special categories of personal data (sensitive data) (see section 8 below), more stringent regulations apply. The processing of such data is prohibited, unless one of the exemptions applies. Two important general exemptions are that the data subject has publicised the data him or herself (for instance, in the case of a homepage and only in so far as the data relate to the data subject him or herself) or if the data subject gives his or her express consent to publication. The Wbp also includes a specific exemption from the prohibition relating to the processing of sensitive data for scientific research or statistics (and therefore not for general historical purposes!), but only provided that four conditions are fulfilled:

1 The research is in the public interest;
2 The processing of the sensitive data is necessary for the research in question;
3 Requesting express consent would prove impossible or would require disproportionate efforts.
4 Sufficient safeguards are put in place during the research, to the extent that the privacy of the data subject is not disproportionately prejudiced.[24]

An archive of Internet pages containing personal data may therefore be constructed for scientific purposes and may be made accessible to a restricted group of scientists via terminals in the library, however this does not automatically mean that the archive can be published on the Internet. Moreover, not all scientists can automatically be given access to the electronic material. The heritage institute must test each specific research request against the four requirements mentioned above.

The Juridische Wegwijzer Archieven en Musea [Legal Companion to Archives and Museums] online therefore justifiably concludes that: *The processing of sensitive data within the scope of making heritage available electronically cannot be easily reconciled with the Wbp. The provision of sensitive data to a large, undetermined public is problematic; the exemption for the purposes of scientific research does not accommodate institutes that wish to publish their material widely.*[25]

8 What constitutes *sensitive* data?

The Wbp makes a distinction between 'normal' and 'special' (sensitive) categories of personal data. Sensitive data are data relating to a person's religion or personal beliefs, race, political persuasions, health or sexual orientation, as well as personal data relating to the person's membership of a trade union. Sensitive data also include personal criminal data and personal data relating to unlawful or objectionable behaviour in connection with an imposed prohibition due to that behaviour. It is important to note here that the term 'criminal data' comprises information regarding convictions as well as regarding suspicions that are more or less founded. The fact that somebody is arrested or that an official report has been compiled against him or her due to a specific offence is also considered to be an item of criminal data.

23) Publication of search terms is risky however, which was proved when AOL published a large number of search results in August 2006, after the American judicial authorities requested them. It turned out that the search terms also included personal data, such as the names of people who searched for themselves.
24) Article 23, paragraph two of the Wbp.
25) Annemarie Beunen and Tjeerd Schiphof, Juridische Wegwijzer Archieven en Musea [Legal Companion to Archives and Museums] online, commissioned by the Taskforce Archieven en Museumvereniging [Archives and Museums Association Taskforce], 2006, page. 44.

Sensitive data are subject to a more stringent legal regime than other forms of personal data. Processing of sensitive data is prohibited[26], unless the data subject has given his or her express consent, or if the data subject has consciously publicised the data him or herself.

8.1 Exemptions from the prohibition relating to the publication of sensitive data

Those who wish to publish sensitive data on the Internet anyway may utilise one of the two aforementioned exemptions from the prohibition to process sensitive data: the express consent of the data subject, or the fact that the data has been consciously publicised by the data subject him or herself.

8.1.1 Express consent

By adopting the term 'express consent', the Wbp imposes a strict requirement with regard to the quality of the consent. Such consent is not permitted to be implied or tacit; the data subject must have expressed his or her desire to grant consent for publication of the data relating to him or her in speech, writing or through his or her behaviour.[27] The express consent can therefore not be replaced by providing the opportunity to have the data deleted (also referred to as an 'opt out').

8.1.2 Publicised by the data subject him or herself

Any adult who deliberately publishes information about him or herself on a personal homepage or weblog under his or her own name, such as reports of medical problems, clearly publicises this information him or herself. This makes the prohibition on collecting and processing these sensitive data void. The issue of whether someone has publicised sensitive data sometimes depends on the intention of the data subject. A politician who stands for election clearly publicises his or her political persuasions. The same applies to an imam, who, as an imam, gives speeches in public on the Islam. This does not apply, however, to reporting ill or a physical handicap. Although a physical handicap is frequently visible to one and all, the data subject does not publicise this item of data regarding his or her health of his or her own free will. The data is therefore not permitted to be processed, unless the data subject actively calls attention to this in public, for example, if he or she is an advocate of a patients' association.

8.2 Imagery

Photographic, video and sound recordings of recognisable natural persons are also classed as personal data.[28] The term 'recognisable' in relation to such recordings is more comprehensive than the term 'directly identifying'. Even if the face of the data subject is obscured, for example, with a black stripe, a photograph may constitute an item of personal data. This is, for example, the case when publishing camera images of alleged shop lifters. It is possible that the data subject will be recognised by their friends, acquaintances or neighbours, based on their appearance, hair style and clothing.[29]

PHOTOGRAPHS OF PUPILS

A primary school decides to place the photographs from a school trip on the school's website. In doing so, the school must observe the regulations under the Wbp. In particular, the school must obtain the express consent of the children's parents. The parents may later withdraw this consent at any time. In this case, the school will in principle be required to delete the images of the data subject.

If a person publishes image material of him or herself, he or she grants consent to publication in this context. This means that there are legitimate grounds for such action, also for the owner of the website on which the material is published. If an individual wishes to publish images of another natural person on the Internet, he or she must have received the consent of the data subject or be able to demonstrate that there is a necessity for such publication (see II.4). Special attentiveness is only required if a controller is publishing photographs or other images with the express aim of making a distinction according

26) The legal exemptions are described in Articles 17 to 22 inclusive of the Wbp, such as the internal use of data regarding membership of a political party, trade union or church by the organisation in question or the use of medical data by social workers, if that is necessary in order to treat or care for a data subject correctly. In principle, none of these exemptions apply to the (open) publication of personal data on the Internet.

27) Explanatory Memorandum, pages 122-123.

28) Directive 95/46/EC, Consideration 14: 'Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data.'

29) Opinion 4/2007, Example No. 19: Publication of video surveillance, page 21.

to race. In this case, the Dutch DPA considers it a reasonable application of the law to regard the imagery as a special category of personal data. The processing of such data is prohibited, unless one of the abovementioned exemptions applies. Publications that are intended solely for the purposes of journalism or for the purposes of literary or artistic expression (see Chapter 4 of these guidelines) are subject to less stringent rules with regard to the processing of image and sound material. In addition to this, the Wbp does not apply to the publication of imagery on the Internet exclusively for personal or household purposes. On the basis of this exemption, private individuals can therefore, for example, freely publish family photos on the Internet, provided that access to such data has been restricted to a clearly pre-defined group of persons. The same applies to photographs on profile sites. If the profile is blocked from search engines and access is limited to friends or acquaintances, publication under these circumstances falls under the personal/household exemption. The Wbp therefore does not apply in any way.

8.3 Identification numbers

Identification numbers constitute a separate category of sensitive data. Since personal identification numbers facilitate the linking of various files, they constitute an additional threat to privacy. In accordance with Article 24 of the Wbp, mandatory numbers for the identification of persons may only be used in order to implement the Act in question or for objectives laid down in the Act. In practice, this means that the publication of a person's social security number (which is soon to be called a Citizen's Service Number) on the Internet is prohibited, even if the data subject has given his or her consent.

II

OBLIGATIONS OF THE CONTROLLER

1 Introduction

Unlawful publications of personal data must be removed from the Internet immediately by the controller. Prior to the publication of personal data on the Internet however, a controller must take a number of steps in order to avert unlawful data from being published. This chapter of the Guidelines includes instructions for the controller in order for him or her to comply with the requirements of the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act] in the stages prior to, during and following publication.

As will be explained below, the controller must determine, prior to publication, whether the publication serves a legitimate purpose and whether that purpose is compatible with the objective for which the data were originally obtained. Preferably, the controller must ask for the consent of the data subjects, otherwise, he or she must be able to substantiate that publication is permitted by virtue of one of the other statutory regulations relating to the necessity of publication.

Upon publication, controllers must actively inform the data subjects of the purpose and intention of the publication. In addition, all controllers must clearly state their own identity in a manner that is accessible to each person who visits the publication. Personal data is not permitted to be retained nor made available for any longer than is strictly necessary. Moreover, the controller must actively guarantee the quality and accuracy of the personal data that is published. One last important step that controllers must take in order to comply with the requirements of the Wbp is to take security measures against unauthorised use.

Finally, following publication controllers must be aware of the continuing obligation to introduce amendments, for example, in the event that a data subject withdraws his or her consent to publication, or if the data appear to be unlawful.

PRIOR TO PUBLICATION

2 Legitimate purposes

Anyone who wishes to publish personal data relating to third parties on the Internet must ask him or herself whether the data are being collected and used for a legitimate purpose. Article 7 of the Wbp states that personal data may only be collected for clearly defined, explicitly specified and legitimate purposes. A purpose may, for example, include: replacing of a hardcopy club newsletter by a publication on the Internet, with the purpose of informing the members of an association about the activities of that association. A purpose is not permitted to be so vague or liberal that there is no framework by means of which to test whether the data actually are necessary for the purpose stated.

3 Further processing

When publishing data on the Internet that were collected for another purpose, the controller must determine whether publication on the Internet is consistent with the initial purpose. Article 9 of the Wbp imposes an obligation to assess the compatibility of the further processing with the original purpose and provides five criteria that must be taken into account in all cases:

a The relationship between the purpose of the intended processing and the purpose for which the data were obtained;
b The nature of the data in question;
c The consequences of the intended processing for the data subject;
d The manner in which the data were obtained;
e The extent to which appropriate safeguards have been taken in respect of the data subject.

DATA RELATING TO FORMER PUPILS

A school for secondary education asks all pupils whether they wish to continue providing the school's administrative department with accurate contact details after their final examination, such as their address, telephone number and e-mail address. The school specifies the organisation of future reunions as its purpose, as well as being able to send other information with regard to school anniversaries. The school is frequently approached by former pupils seeking contact with former classmates and so it decides to publish the contact details of all of its former pupils on the Internet, so as to enable them to contact one another more easily. This method of operating contravenes the principle relating to the purpose relationship in the Wbp, because the data were collected for a different purpose and publication of the data on the Internet could have unpleasant consequences for the data subjects. The publication of contact details on the Internet may, for example, lead to data subjects receiving spam or to unsolicited contact with other former pupils, but also, in a more general sense, to the formation of judgments by third parties with regard to a person's qualities in relation to the quality and nature of the school in question. If the school wishes to offer former pupils the opportunity to contact one another, they must choose another way in which to do so, for example, by means of requesting their express consent when collecting the data. Even with such consent, it is important that the school puts suitable safeguards in place, such as blocking of the data by means of a (unique) password and blocking of the pages from search engines.

3.1 Re-use of personal data from other publications

Many people use data from other websites in personal publications, such as photos in which the people are recognisable, or addresses. The Wbp however stipulates major restrictions in relation to re-use. The fact that personal data are on the Internet does not mean that they can simply be re-used in another context for a different purpose. The new purpose must be compatible with the original purpose and the controller must have an independent ground for the publication, which renders the publication legitimate. Someone who, for instance, maintains a weblog that incorporates sensitive data about his or her person, such as a description of health problems, is publicising this data him or herself. Re-use of sensitive data is not prohibited in the event that the data subject has publicised the data him or herself, however, any controller who wishes to process these data in a personal publication must have an independent ground that renders the publication legitimate (see section 4 below: asking for consent or demonstrating necessity).

The requirement for compatibility of the Wbp overlaps with many stipulations in the Act with regard to the quality and security of data. Even if the new purpose is compatible with the previous purpose, the processing may be considered to be unlawful, for example, if the data to be copied comprise obsolete, incorrect information regarding a person's job or career. The topics of quality and security will be discussed in greater detail in sections 7 and 8 of this chapter. Another provision that applies is the general principle (of Article 6 Wbp) that controllers exercise due care and attention when collecting and processing personal data. This stipulation most certainly plays a major role during the assessment of the compatibility of publications on the Internet.

3.2 Re-use of personal data by third parties

During the assessment of whether (re-)publication of personal data on the Internet is compatible with the original purpose, a controller must not only account for the origin of the data, but also for the risk of others using the data that the controller him or herself publishes on the Internet. In order to reduce the risks to data subjects, each controller must take adequate security measures against illegitimate re-use.

For a correct risk assessment, the role of search engines must be taken into account. Publications on the Internet that are actually aimed at a small audience are made accessible worldwide by search engines. Search engines can link widespread information of various types about a single person. This may create a new picture, with a much higher risk to the data subject than each of the separate items of data. Strict containment of the range of possibilities for use and blocking of personal data from search engines therefore form important measures to be used in order to prevent illegitimate re-use. This requirement is specified in greater detail in section 8 of this chapter.

3.3 Obligation of confidentiality

The Wbp prohibits publication of personal data, if the data fall under an obligation of confidentiality by virtue of a position, occupation or statutory regulation.[31] This provision is frequently implemented in cases in which medical professional secrecy plays a role, yet was also used by the Dutch DPA when assessing a government initiative to publish personal data on the Internet.

PUBLICATION OF DATA IN RELATION TO THE VALUE OF REAL ESTATE

In 2003, the Ministry of Finance requested the recommendation of the Dutch DPA in relation to a number of intended amendments to the Wet waardering onroerende zaken (Wet WOZ) [Valuation of Real Estate Property Act]. The proposal concerned the intention to enhance the disclosure of data relating to the value of immovable property by placing valuation reports on the Internet. The Dutch DPA recommended that[32] : 'In view of the foregoing, the Dutch DPA has come to the decision that general accessibility of valuation data on the Internet would not be in keeping with the Wbp and the Wet WOZ. The Dutch DPA endorses the judgment of the Raad van State [State Council] that the value data relates to sensitive information. For that reason, on the basis of Article 40, paragraph one of the Wet WOZ and Article 9, paragraph four of the Wbp, further processing of these data (by placing the data on the Internet) needs to be refrained from.

4 Asking for consent or being able to demonstrate necessity

Controllers that wish to publish personal data on the Internet are subject to an obligation to require the consent of the data subjects, unless there is another necessity for the publication that can be demonstrated, such as compliance with a statutory obligation or the performance of a contractual obligation. The Wbp lists this as a legitimate ground for processing data. In total, Article 8 of the Wbp lists six legitimate grounds.[33] In the event that consent has not been granted (Article 8, subsection a of the Wbp), publication is only permitted in the event that it is necessary in accordance with one of the following five legitimate grounds for publication:

- For the performance of an agreement in which the data subject forms one of the contracting parties, or in order to take pre-contractual measures in response to a request from the data subject and which are necessary in order to conclude an agreement (Article 8, subsection b of the Wbp.)
- In order to comply with a statutory obligation that the controller is subject to (Article 8, subsection c of the Wbp).
- For the protection of a vital interest of the data subject (Article 8, subsection d of the Wbp).
- To enable the relevant administrative body or the administrative body to which the data are disclosed to correctly perform a task under public law (Article 8, subsection e of the Wbp).
- In order to uphold the legitimate interests of the controller, or of a third party to which the data are disclosed, unless the interests or the fundamental rights and freedom of the data subject take precedence, including, in particular, the data subject's right to the protection of his or her privacy.

Each of the legitimate grounds for publication is explained in detail below.
Additional regulations apply in relation to sensitive data, such as criminal data. The processing of such data is prohibited, unless the data subject has clearly publicised the data him or herself, or has given his or her express consent for the data to be processed (see Chapter I, section 8). The lifting of the processing prohibition does not release the controller from his or her obligation to have an independent legitimate ground for the publication.

4.1 Consent

Consent, the legitimate ground for many publications on the Internet, must be unequivocal (and in the case of sensitive data, even 'express'). The controller is not permitted to adopt the principle 'silence lends consent', but must rule out any doubt with regard to the issue of whether the data subject has given his or her consent, and for what specific type of processing the controller has obtained consent. If

31 Wbp, Article 9, paragraph 4.

32 Dutch DPA, z2003-01563, 11 February 2004, URL: http://www.cbpweb.nl/documenten/adv_z2003-1563.stm

33 For a general explanation of Article 8 of the Wbp, see the fact sheet intended for controllers *Disclosing personal data*, and the fact sheet intended for data subjects *Disclosure of your personal data*, both of which are available to download from the Dutch DPA's website, URL: http://www.cbpweb.nl, under 'News and publications', 'Fact sheets'.

the publication is a publicly accessible discussion forum or guest book on the Internet, the controller does not however need to request explicit consent in order to publish a response; he or she may, within reason, assume that the data subject understands that the response will be published on the Internet.[34)]

CENTRE FOR WORK AND INCOME (CWI) PUBLISHES JOBSEEKERS' DATA ON INTERNET

In response to messages in the media in April 2004, reporting that personal data relating to jobseekers were freely accessible on the vacancy site 'werk.nl', the Dutch DPA requested that the Centrum voor Werk en Inkomen (CWI) [Centre for Work and Income] clarify the issue. From the information that was provided, it appeared that the jobseekers were able to decide for themselves whether, in addition to data relating to their education and work experience, they also wished to place other personal data (such as their name, address details and telephone number) on the Internet. The privacy statement of the CWI clearly stated that these data were openly accessible to others. The CWI has since however introduced measures to restrict access to jobseekers' data. Only employers with a so-called employer's account can now directly request all of the data relating to jobseekers. [35)]

4.1.1 Withdrawing consent

A data subject who has at a certain point given consent to processing of his or her data may withdraw that consent at any time.[36)] For the sake of completeness, the Explanatory Memorandum to the Wbp also adds that such withdrawal will have no consequences for processing of the data that has taken place prior to the moment of withdrawal.[37)] This curtailment however bears no relation to the continuation of the publication of personal data on the Internet. From the moment that consent is withdrawn, the publication becomes unlawful, unless the controller can justify processing the data by means of another legitimate ground for publication. That means that controllers must introduce technical measures in relation to publications on the Internet, in so far as these are based on consent, so that personal data can actively be deleted if a data subject withdraws his or her consent.

4.1.2 Consent provided by persons under the age of sixteen years

The Wbp imposes special regulations in relation to persons under the age of sixteen years. In order to process personal data relating to young people under the age of sixteen years, controllers must obtain the consent of either the young person's parent or their legal representative(s). The controller must be able to demonstrate that he or she has obtained the parents' consent. If that is not the case, the consent of the young person in question is void, thereby rendering the publication of the personal data on the Internet unlawful.[38)]

It is a daily routine for young people to publish detailed information about themselves and their friends and acquaintances on the Internet, for example, on their own website or in social network environments. Provided that the data subjects do not find such publications bothersome, the statutory requirement for consent may sometimes therefore seem meaningless. When publishing on the Internet however, the controller must take into account the fact that the consequences may only become perceptible many years later, due to the linking of data relating to a person over the years, or due to the fact that a young person may want to be able to develop in a different way to previously within a new environment (for example, when changing schools).

The limit of 16 years imposed in the Wbp means that the owners of websites or network environments that are aimed specifically at people under the age of 16 years, have a social responsibility to point those young people to their rights and obligations, in a manner that is both clear and understandable to the target group.

34) '(...) knowledge which, by virtue of social views, it can reasonably be expected that the data subject possesses.' Explanatory Memorandum, page 66.

35) Dutch DPA, April 2004, z2003-1437, URL: http://www.cbpweb.nl/documenten/uit_z2003-1437.stm

36) Article 5, paragraph two of the Wbp: 'Consent may be withdrawn by the data subject or his or her legal representative at any time.'

37) 'A data subject who has at a certain point given consent to processing of his or her data may withdraw that consent at any time. Such withdrawal will however bear no consequences for the processing of the data that has taken place prior to the moment of withdrawal. This applies to all types of processing. In view of the compulsory character of this regulation, this is explicitly specified in Article 5, paragraph two.' Explanatory Memorandum, page. 67/68.

38) 'Article 3:40, paragraph one of the Burgerlijk Wetboek (BW) [Netherlands Civil Code] specifies that a legal act which, by virtue of its content or purpose, violates morality or public order, is void. With regard to processing data for a specific purpose, consent that has not been obtained lawfully must be viewed as being void.' Explanatory Memorandum, page 67.

RULES REGARDING PUBLICATIONS BY OR FOR YOUNG PEOPLE

Controllers of publications or network environments that are visited frequently by young people must at least comply with the following regulations in order to comply with the Wbp:

1 Emphasise that the users must inform their parents and must ask for their consent.
2 Warn that users are not permitted to publish personal data about others (which are also often minors) without having obtained their consent.
3 Introduce technical measures to limit further processing on the Internet as much as possible, such as blocking of personal profiles from search engines and allowing the user to exercise personal control over which other users of the site or environment have access to his or her data.
4 Strict restrictions upon the type of data that are requested from young persons. Sensitive data relating to minors, such as data regarding their sexual orientation or religious beliefs, must not be published under any circumstances. Controllers are not permitted to assume that young people can fathom the risks of judgment on the basis of such a characteristic..

4.2 Necessity

Besides consent the Wbp comprises five other legitimate grounds for publication, each based on a demonstrable necessity of the controller. These are: to perform an agreement, to comply with a specific statutory obligation, to protect a vital interest, to correctly perform a task under public law or to make a comparative assessment of interests.

4.2.1 Performance of an agreement

The legitimate ground that publication on the Internet is necessary for the performance of an agreement may apply in the case of the provision of a service that involves mediation via the Internet. That may, for example, relate to mediation between jobseekers and employers, or between people who are seeking contacts or a relationship. In view of the obligation to provide information as referred to in the Wbp (see section 5 below) and the stipulations in the Burgerlijk Wetboek (BW) [Netherlands Civil Code] with regard to the accessibility, comprehensibility, reasonableness and fairness of contractual provisions,[39] it is highly important in relation to such services that the data subjects are well informed with regard to which data are published on the Internet, and the extent to which the data are protected against unintentional re-use by third parties, for example, by means of a password and blocking of the personal data from search engines.

4.2.2 Statutory obligation

Having to fulfil a statutory obligation is a legitimate ground for publication that is expected to be used increasingly frequently in the future by government institutions or administrators of public registers. A great deal of legislation is currently being developed to promote the transparency and uniformity of the decision-making process of administrative bodies. Electronic publication of personal data is sometimes an explicit requirement in this process. The Dutch DPA dedicates itself in this respect to establishing a clear distinction between disclosure and publication on the Internet. Being permitted to or even obliged to disclose personal data does not automatically mean that publication of the data on the Internet is permitted.

The distinction between a statutory obligation to collect specific personal data and the publication of such data on the Internet played a major role in an investigation carried out by the Dutch DPA in 2005 into the publication of (applications for) construction permits on the Internet by the municipality of Nijmegen. All kinds of personal data need to be entered on the municipal application form, such as the applicant's name, address, e-mail address, telephone number, signature and the total of the building costs. The municipality scanned the application forms and published them on the Internet. The Dutch DPA decided that a statutory obligation to maintain a register of building permits did indeed exist, but that there was no statutory obligation to publish all of the documents in their entirety on the Internet.

39) The obligation to provide information to consumers was tightened in the 1990s in accordance with various EU Directives. In the Netherlands, the tightened provisions were elaborated upon in Articles 233 and 234, Book 6 of the BW, concerning the delivery of general provisions and in Articles 236 and 237, Book 6 of the BW, concerning unreasonable conditions.

The Dutch DPA wrote: *This does not automatically justify the fact that all of the personal data used by the municipality in the procedure for granting the construction permit – data that are recorded in the register of building permits with good cause – were included in the Digitaal Bouwarchief [Digital Construction Archives], which is accessible via the Internet. In theory, the fact that the municipality is permitted to record this data out of necessity (in the analogue archive, ed.) does not mean that the municipality is also permitted to disclose these data to third parties, regardless of whether restrictions are in place.*[40)]

4.2.3 Vital interest

The legitimate ground of claiming that publication is necessary for the protection of a vital interest of the data subject relates to a medical necessity. The intention of this article is to be able to save lives in acute emergencies, if, for example, the data subject is unconscious. It is highly improbable that this legitimate ground for publication can be used to justify a publication on the Internet.

4.2.4 Effective fulfilment of a task under public law

Government institutions and services that wish to publish personal data on the Internet can avail themselves of the legitimate ground for publication included in Article 8, subsection e of the Wbp. One of the legitimate grounds is if publication is necessary in order for the relevant administrative body to effectively perform a task under public law. In that respect, each item of data to be published must be considered carefully. The fact that disclosure of certain data to an administrative body is necessary, does not justify the fact that all of the data are also automatically published on the Internet. This also applies to administrative bodies that consider active disclosure within the framework of the Wet openbaarheid van bestuur (Wob) [Government Information (Public Access) Act].[41)]

4.2.5 Legitimate interest

One last legitimate reason for publication lies in the consideration of the individual justifiable need for publication against the rights and freedom of the data subject, particularly the right to the protection of his or her privacy. This consideration is much more general in nature than the first five legitimate grounds for publication and, due to its nature, is dependent on the circumstances of a specific publication. In principle, only a few publications will be able to plead this legitimate reason, because publication on the Internet carries unforeseeable risks for the privacy of data subjects.

A controller who wishes to rely on Article 8, subsection f of the Wbp must first of all demonstrate that an intended publication is necessary for the fulfilment of a legitimate interest. In accordance with the case law of the European Court of Human Rights (ECHR), necessity is not the same thing as 'good' or 'useful'.[42)] Moreover, the controller must demonstrate that the intended interest cannot be served in a different way or by less drastic means.[43)]

Once this has been considered, the controller must consider a second aspect, in which the individual interests of the data subject form an independent weight in the scale. A controller cannot suffice with the argument that the data are already available on other sites on the Internet and that the infringement contained within the new publication would therefore only be minor.

The Explanatory Memorandum to the Wbp provides four questions to assist controllers in making the two comparative assessments.

- Does an interest that justifies processing personal data truly exist?
- Does processing the data constitute an infringement upon the interests or fundamental rights of the person whose data are being processed, and if so, should, depending on the seriousness of the infringement, processing of the data not be omitted?
- Can the purpose for which the data are being processed also be achieved by other means, i.e. without the need for processing to take place?

40) Dutch DPA, z2005-0212, 1 December 2005, URL: http://www.cbpweb.nl/documenten/uit_z2005-0212.shtml

41) In view of the privacy aspects of active disclosure in the near future, the Dutch DPA will publish policy regulations with regard to the connection between the two laws Wob and Wbp.

42) ECHR 25 March 1983, Silver and others v. United Kingdom, no. 97: '(a) the adjective 'necessary' is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable […].'

43) In accordance with the established case law of ECHR, such a consideration of interests must be in keeping with the principles of proportionality and subsidiarity. The latter means that invasion of the data subject's privacy must be proportional to the intended purpose and that this cannot be achieved by less drastic means.

- Is processing to the extent intended proportionate to the intended purpose?[44)]

This comes down to the fact that the controller has to ask him or herself:
– Is publication truly necessary? Is there no other way?
– Does the interest of publication weigh up against the disadvatages?
– What does the publication mean for each individual data subject in his or her specific case?

A controller must provide insight into the result of these considerations. The result of the consideration must be a clear interest that is socially acceptable and is not contrary to that which is becoming in society, according to written and unwritten law. The controller is not permitted to swiftly allow the interests of processing to prevail above the interests of the data subject, due to the risks of further processing as a result of publication on the Internet.

The fact that the interests of data subjects carry a great deal of weight and often take precedence above the interests of data processing is something that has been proved in case law regarding the public display of photographs of alleged shoplifters. In August 2004, the judge of the Amsterdam District Court in interlocutory proceedings[45)] decided that a shopkeeper was not permitted to pin up a photograph of a woman in his shop, who he believed to be a shoplifter. The publication would contravene the Auteurswet [Copyright Act], but also the Wbp, particularly Article 8, subsection f. *The posting of the photograph of [claimant] with the adjoining text 'This woman committed theft in this store', is also in violation of the Wbp. The video images recorded with a surveillance camera can be considered as a file in the sense of Article 1, paragraph c of the Wbp, now that there is a structured whole of personal data. The processing of these data by a shopkeeper falls within the scope of the Wbp. From that which has been considered above (....), it follows that [claimant] did not provide unequivocal consent to the processing of the video images into a photo – as required under Article 8, paragraph a of the Wbp – and that the interests of [claimant] take precedence in the consideration of interests referred to in Article 8, paragraph f of the Wbp.*[46)]

The judge in interlocutory proceedings also considered (in point 9): *"A publication such as the one under discussion, which comprises an element of punishment, constitutes taking the law in respect of [claimant] into one's own hands." He also added: "Tracking down and trying suspects is the exclusive right of the judicial authorities and it is not up to the citizens to publicly disgrace potential suspects."*

Two years later, when the contested photo was once again published in a newspaper, the Dutch DPA issued a general decision with regard to the admissibility of private companies publishing photographs of persons suspected of being shoplifters.[47)] The Dutch DPA was of the opinion that the Wbp does not permit shopkeepers to publish and display photographs of persons suspected of shoplifting in shop windows or in other locations that are visible to the public.

The judgment was that: *The use of the images for publication in shops, so that the accused is in fact subjected to public shaming for criminal offences, cannot be considered a socially acceptable purpose. This entails that it cannot be considered a legitimate interest on the part of the controller.*[48)]

DURING PUBLICATION

5 Obligation to provide information

The Wbp comprises an obligation to provide information. Controllers of publications on the Internet must, on their own initiative, provide an insight into the purpose of the publication, how and which personal data they are processing and their identity. This is not a once-only obligation, but applies in respect of each person whose data they are processing.

44) Explanatory Memorandum, page 86.
45) LJN: AQ7877, Amsterdam District Court, KG 04/1566 SR
46) Same, under point 12.
47) Dutch DPA, 30 May 2006, z2005-0846, URL: http://www.cbpweb.nl/documenten/uit_z2005-0846.shtml
48) Dutch DPA, 30 May 2006, z2005-0846, page 3.

The obligation to provide information applies if the controllers collect the data themselves (Article 33 Wbp), but also if they obtain the data by other means, for example, by adopting data from other publications on the Internet (Article 34 Wbp). Anyone who collects data on the Internet and wishes to re-use those data in a personal publication must inform each individual data subject that there is a new controller who is processing their personal data.[49] If there are few risks involved in the publication and if the data subjects are reasonably aware of in which context specific personal data about them are published on the Internet, a controller can suffice to send passive information regarding his or her identity and the purpose of the publication, for example, in the form of a privacy statement. In all other cases, a controller must inform all data subjects in advance and provide as much supplementary information as is necessary in order to ensure that the data subjects understand the purpose and how they can oppose publication if they wish to do so.

ADDITIONAL INFORMATION AND ATTENTION WITH REGARD TO PRIVACY AND YOUNG PEOPLE

Young people constitute a particularly vulnerable group when it comes to personal data and the Web. Services on the Web that process data about young people and personal data posted by young people must therefore take extra care to ensure that this personal data is treated with the utmost confidentiality. On the one hand, it is young people who are most likely to identify and exploit the possibilities of new communication techniques and services. On the other hand, most young people do not yet have a proper understanding of the potential consequences of publishing and handing over personal data. This applies to data about themselves as well as data about other young people that they publish. Young people also have an obligation to treat personal data with due care. Controllers must therefore devote particular attention to information on the processing of personal data and ensuring that users are properly informed.

5.1 Scope of the obligation to provide information

How precisely controllers can comply with the obligation to provide information as laid down in the Wbp, is dependent upon a number of factors. The Explanatory Memorandum to the Wbp states that controllers must supply as much information as necessary in order to guarantee that, in each specific case, due care and attention is exercised when the data are being processed, whether the data have been collected personally from the data subject, or indirectly.[50] That means that the scope of the obligation to provide information depends on the controller, the nature of the risks involved in the publication and the way in which the personal data are obtained. Controllers that publish on the Internet with the consent of the data subjects and that have blocked the personal data from re-use by search engines, need only provide a concise statement of their identity and the purpose of the publication prior to publishing the data. Anyone who wishes to publish data on the Internet for a different legitimate reason, such as in order to correctly perform a task under public law, must provide each individual data subject with much more detailed information, particularly if it is not clear beforehand that the data are also being published on the Internet, and must inform the data subjects of their right to oppose publication. The active obligation to provide information only lapses in the event that the controller can demonstrate that informing the data subjects individually would require disproportionate efforts – which is understood to mean that informing the data subjects would involve substantial costs, would require extraordinary efforts to find them, or that attempts to find them would be impossible due to technical problems – and in the event that there are no other means by which the data subjects can be informed using more general channels. In that instance, however, the controller must record from whom and in what way he or she obtained the data, for example, from which other Internet publications the data were taken.

5.2 Obligation to provide information to residents from outside the EU

The obligation to provide information applies to all data subjects whose personal data are being processed, even if the data subjects are residents of a country outside of the European Union. If, for example, a controller wishes to publish a contact list of people from across the world with a highly specific interest, he or she must inform each individual data subject prior to publication. If a resident of the

49) For a general explanation of the obligation to provide information, see the fact sheet intended for controllers Obligation to provide information, which is available on the Dutch DPA's website, URL: http://www.cbpweb.nl, under 'News and publications', 'Fact sheets'.
50) Explanatory Memorandum, page 149-150

WRITING ABOUT WELL-KNOWN PEOPLE

A minister talks about his private life on television. Numerous personal, non-journalistic weblogs devote attention to his statements and all kinds of people then leave comments. As, in this case, the minister made his statements in public, it may be assumed that he is aware of the fact that this will be discussed further in public, including on the Internet. The owners of the weblogs therefore do not need to separately inform the minister that they are processing his personal data. A (non-journalist) controller that avails him or herself of this occasion to publish all kinds of other private information regarding the minister on the Internet, however, including, for example, photos of his family, must indeed thoroughly inform the minister. In view of the potential consequences for the other family members, the issue of whether such a publication can be justified at all is highly debatable.

United States of America notices that his name is on the website in question, without having been informed in advance, he may, in the Netherlands, take recourse to the legal remedies accorded to him in the Wbp.[51)]

5.3 Privacy statement

Controllers wishing to publish personal data on the Internet on the basis of consent no longer need (after having been granted consent) to inform each separate data subject of their identity and the purposes of the processing. A good way in which to fulfil the obligation to provide concise information is to publish a privacy statement. The statement must be drawn up in clear, comprehensible language, must be easily retrievable and preferably, accessible from within each section of the publication.

Following the recommendation of the Article 29 Working Party with regard to the collection of data online[52)], a privacy statement for a publication on the Internet must include the following elements at the very least:

1 The identity, the physical and electronic address of the controller processing the data.
2 The purpose(s) of the processing for which the controller is processing data via an Internet publication.
3 A statement with regard to whether the disclosure of certain information is obligatory or optional.
4 The recipients or the categories of recipients of the collected information.
5 A statement of the data subjects' right, depending on the situation, to grant consent or object to processing of personal data and of the conditions that apply in that respect; a statement of the right of access to and correction and deletion of data. In this regard, the controller must make it clear which person or service the data subjects must approach in order to exercise these rights.
6 The name and address (physical and electronic) of the service or person who is responsible for answering questions in relation to the protection of personal data.
7 Information regarding the use of any automatic data collection procedures (for example, for the recording of IP addresses of visitors to a website or the use of cookies).
8 Information regarding the level of security of a publication during all processing stages (important in the case of publications for a restricted target group), including clarification of whether data can be indexed by search engines, and if so, to what extent.
9 A statement of the retention period for personal data, including any rules of play with regards to exclusion/blacklisting.
10 If applicable: the notification number used when notifying the Dutch DPA of the processing.

The appendix to these Guidelines includes a model privacy declaration that satisfies these conditions. This is a model that can be used for a discussion forum, in which participants may or may not use a pseudonym when publishing their contributions and the legitimate ground that justifies processing the data is consent.

51) Explanatory Memorandum, page 193: 'This means that, when personal data are being collected on data subjects that are located, for example, in the United States, those people must also be informed in the sense of Articles 33 and 34 of the legislative bill. Should anyone notice in any way whatsoever that personal data relating to him or her have been processed in contravention of this regulation, for example, as a result of receiving advertising material that is addressed specifically to him or her, he or she may take recourse in the Netherlands to the legal remedies granted to him or her by this Act.'

52) Article 29 Working Party, WP 43, Recommendation on certain minimum requirements for collecting personal data on-line in the European Union, approved on 17 May 2001.

5.4 Notification of identity

Paragraph two of Articles 33 and 34 of the Wbp stipulates that controllers must make their identity known. This enables data subjects to exercise their rights effectively and to contact the controllers directly. The recommendation of the Article 29 Working Party in 2001 with regard to the collection of data online emphasises the fact that when confirming his or her identity, the controller must specify both an electronic and a physical address. The directive on electronic commerce (2000/31/EC) also comprises a similar absolute identity requirement, which has been transposed in Article 3:15d of the Burgerlijk Wetboek (BW) [Netherlands Civil Code].[53] Such an absolute identity requirement carries risks however for the privacy of individual web loggers (bloggers) or critics. A natural person may have good reasons for not wanting to publish his or her physical contact address on the Internet, for fear of threats or other types of unsolicited approaches.

The recommendation of the Article 29 Working Party primarily focuses on controllers that collect and process data in a professional manner, for example, for the purposes of direct marketing or other commercial services. At the time, the Working Party had probably not foreseen the possibility that masses of individuals would start to publish personal data on the Internet. The directive on e-commerce does not focus on natural persons, but on commercial service providers that perform their services 'for remuneration, as a general rule'.[54] In the case of publications by natural persons, a further consideration is necessary in order to do justice to the good reasons that a controller may have for not wanting to publish his or her physical address on the Internet. For that reason, the Dutch DPA considers it a reasonable application of the law if a natural person that publishes on the Internet with no commercial objective limits him or herself to publicising an electronic address. Two conditions apply in that respect:

- The controller is easily accessible for data subjects by means of an electronic e-mail address.
- This e-mail address is issued by a provider located in the Netherlands.

In the case of such controllers (who are publishing as private individuals and with no commercial objective), it will not suffice to state a (frequently free) e-mail address provided by a service provider operating at an international level, such as Microsoft, Google or Yahoo. Such an e-mail address can make it unnecessarily complicated for a data subject to obtain justice if a controller does not provide an adequate response.

The e-mail address must have been issued by a provider located in the Netherlands, within the Dutch .nl domain. Controllers who possess their own mail server can also fulfil this obligation, provided that they process the e-mail under the .nl domain. The requirement of having an electronic contact address in the .nl domain makes it easier for the data subjects to take further steps to discover the identity of the controller. The Lycos judgment of the Amsterdam Court of Appeal[55] can serve as a reference point for the data subject when speaking to the provider if the controller does not make his identity known for a publication on the Internet and is therefore undeniably acting in contravention of Articles 33 and 34, paragraph two of the Wbp.[56]
Private individuals who do not wish to use a Dutch e-mail address are subject to the complete obligation to publicise both a physical and an electronic contact address.

53) 3:15d, paragraph one BW: 'Any person providing a service of the information society makes the following data easily, directly and permanently accessible to persons making use of that service, particularly in order to obtain information or make information accessible:
a. his or her identity and residential address;
b. data that enable him or her to be contacted quickly and allow communication to take place directly and effectively, including his or her e-mail address; (sections c to f inclusive not cited)'.

54) 3:15d, paragraph three of the BW.

55) Judgment of 24 June 2004 of the Amsterdam Court of Appeal, role number 1689/03 KG. The Court judged that hosting provider Lycos had to disclose the personal data of a subscriber to X. The subscriber had branded X as a swindler on his website. The Court judged that it was sufficiently plausible that the statement could be unlawful and that Lycos therefore acted unlawfully by not disclosing the personal data of the subscriber. In late 2005, the Supreme Court dismissed the appeal initiated by Lycos, as a result of which the judgment of the Amsterdam Court of Appeal became final and irrevocable. The Supreme Court commented however that it did not wish to formulate a general measure through this dismissal in relation to the obligation to disclose personal data to third parties. AU4019, C04/234HR.

56) As it happens, the subscriber in this case, it emerged, had provided false contact details. The Court emphasised that an obligation to identify their customers does not exist for suppliers of electronic communications services. The obligation to make a .nl e-mail address available does not therefore provide a waterproof method by which to establish the identity of a controller, but it does however make it easier.

6 Notification obligation

In principle, controllers are obliged to notify the Dutch DPA of all data processing, unless they fall under the Vrijstellingsbesluit [Dutch Data Protection Exemptions Decree] or appoint their own data protection officer (DPO).[57] The notification obligation referred to in the Wbp (and the underlying European Privacy Directive), however, dates back to before the massive increase in weblogs, for example, and other popular Internet publication formats, such as websites of associations and companies. It is questionable whether the legislator intended the notification obligation for the practice of data processing on the Internet in the current form and scope. There are still no specific exemptions for Internet publications at this moment, but these are under development however (see section 6.3 below). Given these circumstances and not withstanding any special circumstances, the Dutch DPA only grants priority to verifying the notification of publications comprising sensitive data (see Chapter I, section 8) and of publications which, from a security perspective, carry major risks for the data subjects, such as the risk of identity fraud.

6.1 What does notification mean?

A notification to the Dutch DPA includes a description of one or several data processing operations. Article 27, paragraph one of the Wbp lays down an obligation to provide notification of the intended processing operations, that is to say that the notification must take place before proceeding to process data. Because 'processing' also relates to the collection, this means that the controller must notify the Dutch DPA of the processing to be carried out before he or she obtains personal data.[58] The notifications will be included in a public register, which is freely accessible via the website of the Dutch DPA, in accordance with Article 30 of the Wbp. The fact that a notification is included in the public register does not mean that the Dutch DPA has approved the processing or has deemed it lawful. Also, the notification does not provide a guarantee that the controller is processing personal data in accordance with the Wbp.

6.2 Vrijstellingsbesluit [Dutch Data Protection Exemptions Decree]

Many types of well-known, frequently occurring forms of data processing, which do not carry significant risks and of which can be assumde everyone is aware of, are exempted from the notification obligation by the Vrijstellingsbesluit [Dutch Data Protection Exemptions Decree.[59] As a general rule, however, the exemptions do not bear relevance to the publication of personal data on the Internet and so these guidelines do not elaborate upon this issue.

6.3 Future: development of exemptions in relation to Internet publications

In 2007, the Ministry of Justice worked towards the extension of the Vrijstellingsbesluit. It is expected that, in the future, foundations and associations that publish personal data on their websites and private individuals that produce personal publications, will, subject to certain conditions, not need to notify the Dutch DPA of their processing operations. 'Personal publications' is understood to mean publications that are personal by nature, are not being produced for commercial purposes and are compiled for personal use and purposes. A supplementary condition for the new exemptions from notification is that personal data must be deleted immediately if a data subject lodges an objection to the recording of his or her personal data. Moreover, it is important that the pages comprising personal data are blocked against processing by search engines in order to prevent incompatible use.

Educational institutes and companies that publish personal data on a secure intranet are also expected to fall under the new exemptions. The exemption also comprises publication on a secure intranet of photo galleries of employees, students or lecturers, provided that the publication is approved by the

57) For a general explanation of the notification obligation, see the fact sheet intended for controllers Melden en vrijstellingen [Notification and Exemptions], which is available on the Dutch DPA's website, URL: http://www.cbpweb.nl, under 'Nieuws en publicaties', 'Informatiebladen' (only available in Dutch).

58) Explanatory Memorandum, page 137.

59) Decree of 7 May 2001, comprising indications with regard to personal data processing operations that are exempt from notification as referred to in Article 27 of the Wbp (Vrijstellingsbesluit Wbp [Dutch Data Protection Exemptions Decree]), Bulletin of Acts, Orders and Decrees 2001,250, URL: http://www.cbpweb.nl/indexen/ind_wetten_wbp_vrijstellingsbesluit.stm

Works Council. In June 2007, the Dutch DPA was involved in consultations regarding the adaptation of the decree. It is expected that the amendments will enter into force in 2008.[60)]

The exemptions currently being developed relate only to exemption from notifying the Dutch DPA, and not from the obligation to satisfy the requirements in relation to exercising due care when dealing with personal data. The obligation to provide information (and the obligation to disclose the identity of the controller and the purpose of processing the data) remains fully applicable, as do the other stipulations of the Wbp.

7 Quality

The Wbp imposes requirements in respect of the retention period ('lifetime') and the quality of personal data. Data must not refer to identifiable persons for any longer than is strictly necessary and the data must be accurate and relevant.

7.1 Limited retention

Prior to publication of personal data on the Internet, controllers must determine how long they will leave the data online or will continue to retain the data. In accordance with Article 10 of the Wbp, personal data must not be retained in a form that enables the data subjects to be identified for any longer than is necessary for the (justified) purposes stated.[61)] Furthermore, in accordance with Article 11, paragraph two of the Wbp, the controller must make efforts to ensure that personal data are correct and precise. The older the data are, the greater the chance that they are incorrect and could therefore cause unnecessary harm to data subjects. Each time that they publish personal data, controllers must therefore consider which risks the chosen availability period entails. It is advisable to introduce a method whereby personal data can be converted automatically into anonymous data following the expiry of the specified period. Such a procedure was recently recommended by the European Commission.[62)]

7.2 Adequate, relevant and not excessive

In accordance with Article 11 of the Wbp, the controller is only permitted to process data that are adequate, relevant and not excessive in relation to the specified purpose. The Explanatory Memorandum to the Wbp uses the example of a shopkeeper who starts to record persons that he has caught shoplifting. *A shopkeeper, as a general rule, will not need to record which goods the data subject has stolen from his or her shop, but rather the value of those goods.* Furthermore, in this record, he or she is not permitted to store data regarding the (legal) purchasing behaviour of the data subject, because storing such data is excessive in respect of the stated purpose.[63)] The example relates solely to a personal record made by the shopkeeper. A legitimate ground for publishing lists of (supposed) shoplifters on the Internet is not likely to be found in the near future under the terms of the Wbp, due to risks of further processing by third parties.[64)]

60) The Netherlands is not the only country in Europe to decide upon such an extension of the decree; in 2005, France published similar exemptions for Internet publications. See: CNIL, Délibération n° 2005-284 du 22 novembre 2005 décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère personnel mis en oeuvre par des particuliers dans le cadre d'une activité exclusivement personnelle (Dispense n°6) [Consideration No. 2005-284 of 22 November 2005 concerning the exemption from notifying websites distributing or collecting personal data implemented by private individuals in the context of an activity that is exclusively personal (Exemption No. 6)], last amended on 11 May 2006, URL: http://www.cnil.fr/index.php?id=1928 and Délibération n°2006-130 du 9 mai 2006 décidant de la dispense de déclaration des traitements relatifs à la gestion des membres et donateurs des associations à but non lucratif régies par la loi du 1er juillet 1901 (dispense n°8) [Consideration No.2006-130 of 9 May 2006 concerning the exemption from notifying data processing in relation to the management of members and contributors of not-for-profit associations governed by the Act of 1 July 1901 (Exemption No.8)], last amended on 18 May 2006, URL: http://www.cnil.fr/index.php?id=2015

61) For a general explanation of retention periods, see the fact sheet intended for controllers *Bewaartermijnen van persoonsgegevens in uw bestanden* [Retention periods for personal data in your files], and the fact sheet intended for data subjects *Bewaartermijnen van uw persoonsgegevens* [Retention periods for your personal data], both of which are available (only in Dutch) to download from the Dutch DPA's website, URL: http://www.cbpweb.nl, under 'nieuws en publicaties' [News and publications], 'publicaties' [Publications], 'informatiebladen' [Fact sheets].

62) Communication from the Commission to the European Parliament and the Council on promoting data protection by Privacy Enhancing Technologies (PETs), Brussels, 2 May 2007, COM(2007) 228. "Automatic anonymisation of data, after a certain lapse of time, supports the principle that processed data should be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were originally collected."

63) Explanatory Memorandum, page 96-97.

64) See the previously cited judgments relating to the posting up of the photo of an alleged shoplifter, LJN AQ7877, Amsterdam District Court, KG 04/1566 SR and Dutch DPA, 30 May 2006, z2005-0846.

The fact that data must be 'adequate' comprises a duty of care on behalf of the controller to paint as correct a picture as possible of a data subject in respect of whom he or she is publishing personal data. The omission of crucial information can be equally harmful to privacy as listing an excessive amount of private information. For example, omitting the fact that a data subject, whose name features in a list of alleged defaulters, is contesting a claim and on what grounds he or she is contesting the claim, could cause harm to that person.

LAWYER'S ACCESS TO CASE LIST DATA

Lawyers have an interest in access to the case list register of the court in which they litigate. Lawyers gain access to the data of a court in another town via a representative, known as a local counsel. The case list register comprises information relating to all pending civil cases, including a brief profile of the case, the names of the claimant and the defendant, the names of the local counsels and the status of the hearing. In 2002, the Raad voor de Rechtspraak [Council for the Judiciary] decided to introduce a digital case list, 'My Cases ', which enables lawyers to gain access to the case list data from the whole country via the Internet, in the run-up to the abolition of the compulsory office of local counsel, which is currently expected to take place in March 2008.
The Dutch DPA judged this access excessive (did not comply with Article 11 of the Wbp) and that lawyers should only have access to their own cases.[65] The Raad voor de Rechtspraak adapted its policy to this. The access to www.roljournaal.nl has been restricted. [66]

7.3 Accurate

When monitoring the quality of personal data, controllers must also take measures to ensure that data are accurate and are consistent with the truth, without anything having been removed or (wrongfully) changed.[67] A controller who collects and then publishes personal data, must be sure that the data have really been entered or amended by the data subject him or herself and not by a (malicious) third party. Data subjects must not be put in a position whereby they must deny having performed a specific action. If the nature of the publication and the risks that it entails necessitate this, controllers must therefore establish the identity of an applicant or user. There are several means for achieving this, such as biometric applications, PKI Government (the public key infrastructure, in which the government issues certificates to vouch for the identity of a user), DigiD [68] or Open ID (an initiative to ensure correct identification from the bottom upwards, by means of users' trust in one another). Another system, which is used extensively in, for example, Finland and Estonia, is authentication via the infrastructure of Internet banking. [69] Which system can be applied most effectively in the Netherlands to satisfy the security requirements of the Wbp, is dependent upon the reliability and availability of the system, the costs for the controller and the user acceptance.

7.4 Can identity be established by electronic means only?

If the nature of the services and the risks entailed mean that it is necessary to establish the identity of the data subject, the controller must first ask him or herself whether it would suffice to utilise electronic means alone, or whether it is necessary to request confirmation via a separate communication channel in order to exercise the required degree of care. This may be by means of confirmation of a payment

65) The Dutch DPA issued a judgment in respect of this in 2003, in z2002-01015. Following a request for review from the Raad voor de Rechtspraak, the Dutch DPA reiterated its judgment on 20 June 2003, in z2003-0707.

66) See URL: http://www.rechtspraak.nl/Registers/Register+aangemelde+gegevensverwerkingen/#Roljournaal: 'The data may only be consulted by lawyers that have obtained a password for that purpose and for a specific search request that is subject to the approval of the Dutch DPA.'

67) Article 11, paragraph two of the Wbp: The controller takes the necessary measures to ensure that personal data are, in view of the purposes for which they are being collected or will be processed, accurate.

68) DigiD is one of the systems that are currently being developed to establish the identity of a user on the Internet. DigiD incorporates three levels of security: low, medium and high. At the basic level, the combination of login name and password suffices, as used by the Tax and Customs Administration. It has now emerged that this combination is not sufficiently unique, and can also be used by third parties (See the responses to parliamentary questions regarding the use of another person's DigiD when completing a tax declaration, Parliamentary Documents II, 2006-2007, DGB 2007-01961). An additional code is necessary at medium level and is sent by SMS. At the time of laying down these guidelines, this procedure was still not available to companies. For the highest level of security, developments are currently underway for an electronic Netherlands identity card (eNIK). The Ministry of the Interior wants to develop a chip card that each Dutch citizen can apply for at municipal town halls, like a passport. The eNIK enables the holder to notify and verify his or her identity by digital means.

69) Major government institutions in Finland, such as the Ministry of Social Affairs, the Institute for Social Security and the Tax and Customs Administration, have been using the identification system of Internet banking since 2004. See: http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=23144

that takes place at the initiative of the applicant, or by means of the introduction of an offline identification step, such as by letter or by telephone.

7.5 Use of identity papers

It goes without saying that a controller is not freely permitted to request a copy of a data subject's proof of identity in order to establish his or her identity. Passports and identity cards contain two items of sensitive data, the processing of which is, in principle, prohibited, unless one of the statutory exemptions applies. These items of data are, to be specific, the data subject's passport photo and his or her social security number (which will, in the very near future, be replaced by the Citizens Service Number).

DATA FACILITATING EASY IDENTIFICATION

In order to qualify for the status of 'Verified seller' on a mediation website, applicants had to submit an excessive number of documents. According to the Dutch DPA, it would suffice for the controller to request a copy of a recent bank or giro statement and a copy of the person's proof of identity. In addition, the website had to emphatically draw the prospective sellers' attention to the possibility of blacking out all excessive data. Following verification of the person's identity, the copies would have to be destroyed or returned to the potential Verified seller. [70)]

8 Security

Controllers of publications on the Internet must take adequate security measures, especially if the publication includes sensitive data. The risk of re-processing for a purpose other than the one for which the data were originally collected and published must be specifically taken into account when publishing personal data on the Internet.

8.1 Appropriate security measures

Article 13 of the Wbp obliges controllers to take appropriate technical and organisational measures to protect personal data against loss or against any form of unlawful processing. The measures must partly be designed to prevent the unnecessary collection and further processing of personal data.

What can be considered to be an appropriate level of security depends on the status of technology, the type of personal data, the type of processing, the implementation costs for the controller and the expected risks to the data subjects. The legislator has expressly adopted an open standard, without specifying further details with regard to the types of security. *Such details would be very dated and would therefore damage the intended level of security.* [71)]

In order to comply with the security standard laid down in Article 13 of the Wbp when publishing personal data on the Internet, and in view of the current status of technology and the clarification of (legal) norms in previous judgments of the Dutch DPA, controllers must comply with the following five obligations:

1 Avoid unnecessary publication of personal data.
2 Block specific pages containing personal data from search engines.
3 Use passwords or another appropriate method to restrict the target group.
4 Ensure that data transfer is secure by means of the SSL protocol. [72)]
5 Secure machine(s) and underlying databases against unauthorised access by third parties.

70) Dutch DPA, Z2006-00957, 2 March 2007, URL: http://www.cbpweb.nl/documenten/med_20070302_marktplaats.shtml

71) Explanatory Memorandum, pages 98-99.

72) Secure Sockets Layer (SSL) is a standard protocol that makes use of 'public key encryption' technology to provide a secure service between Internet servers, in which the privacy of the communication, the integrity of the communication and the verification and/or the identification of the sender/reciepient are all safeguarded.

8.2 Preventing unnecessary publication of personal data

From the perspective of security, controllers are obliged to take measures to 'prevent unnecessary collection and further processing of personal data' (Article 13 Wbp, third sentence). Sometimes, however, a controller has a thoroughly legitimate ground for collecting and processing specific personal data within the organisation, but that purpose does not lend itself to the integrated publication of these personal data on the Internet. For each item of personal data, therefore, a consideration must be made of the necessity of publication on the Internet, in the light of the expected risks to the data subject. The obligation to minimise data applies in particular to governments and controllers of public registers, because the data subjects in these cases have less opportunity to oppose a specific publication.[73)]

SIGNATURES NO LONGER TO BE PUBLISHED ON THE INTERNET

On 1 May 2007, a new act entered into force regarding the Commercial Register, which comprises provisions in relation to opening the register electronically.[74)] The Act draws a distinction between the compulsory recording of some personal data in the register and the publication of those data on the Internet. Making a record in the register of the Citizens Service Number of the natural persons who have a company, for example, is obligatory, but this cannot be disclosed to third parties and therefore cannot be published on the Internet. Whilst the bill was under discussion in the Lower Chamber, attention was specifically drawn to the risk of publishing the signature of natural persons included in the commercial register on the Internet. The following is an excerpt from the explanation of the amendment, provided by Member of Parliament Van Dijk: *The Chambers of Commerce are increasingly finding that signatures are being copied for the purposes of committing fraud. In that respect, use is made, for example, of the signature noted in the commercial registers, as these can be inspected via the Internet. In order to prevent fraud of this type as much as possible, it is advisable that signatures of natural persons are no longer displayed on the Internet. The Chambers expect that this will raise an effective barrier against the copying of signatures.*[75)] The State Secretary for Economic Affairs immediately adopted the amendment.

8.3 Blocking personal data from search engines

A publication that complies with the Wbp may nevertheless contribute to a data subject's privacy being prejudiced, because third parties can link all kinds of intimate details regarding these data subjects via search engines. Blocking personal data from search engines is free of charge and is a very easy, generally applicable step to reduce the risk of unlawful processing by third parties. All major search engines offer manuals to controllers of publications, with the help of which they can prevent a website or sections of websites from being indexed or archived. [76)]

Without such a measure being in place, major risks arise for the data subjects, as a result of which the publication may be unlawful. Controllers that wish to avoid the risks of unlawfulness therefore block all pages containing personal data from search engines. This can be achieved by means of a general approach, for example by automatically including an anti indexing code in the underlying html, or by means of an individual solution, such as a design in which the data subject gives his or her express consent to the data being accessed by search engines. This second option is useful, for instance, for controllers of profile, photo/video or weblog communities, so that each data subject can make an individual decision with regard to the availability of his or her data to third parties.

73) A specific condition imposed upon government institutions is the Nicolaï motion that was universally adopted when the Wbp was under discussion in the Lower Chamber, in which the government is expressly called upon to use privacy enhancing technologies (PET) within its own systems for the processing of personal data (Parliamentary Documents II, session year 1999-2000, 25 892, no. 31). In the spring of 2007, the European Commission published an announcement in which it emphasised that it is essential that national governments deploy privacy enhancing technologies, including data minimisation, to increase the trust of citizens, both in the set-up of the systems and in the implementation (Communication from the Commission to the European Parliament and the Council on promoting data protection by Privacy Enhancing Technologies (PETs), Brussels, 2 May 2007, COM(2007) 228).

74) Act of 22 March 2007, Regulations relating to a database register of companies and legal entities (Handelsregisterwet [Commercial Register Act] 2007), Bulletin of Acts, Orders and Decrees 153, 1 May 2007.

75) Parliamentary Documents II, 2006-2007, 30656, no. 20, page 7, 12 February 2007.

76) Anyone who wishes to block an entire site from all search engines must place a document entitled 'robots.txt' on the root server with the following content:

```
User-agent:
*Disallow: /
```

The same principle can be applied to each individual webpage, by adding the following code to the header of the page:
<META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">

DELETION OF ACCUSATIONS FROM GOOGLE CACHE

In February 2007, the judge in interlocutory proceedings of the Dordrecht District Court [77] judged that a defendant must make every last effort to have an unjust accusation removed from the Google cache. The defendant was of the opinion that she was swindled and published this on her website. After the payment was credited to her account she removed the accusations, however, the accusations continued to surface via the Google cache. Although the defendant had made efforts to delete the data, a copy was still traceable using the search engine at the time of the hearing. The judge ordered the defendant to delete the statement from the cache of the Internet search engine Google within two days of the court order, under penalty of a €250 payment for each working day that the defendant remained in default.

8.4 Use of passwords or other methods to restrict the target group

Controllers that publish personal data on the Internet with a specific objective must ensure adequate protection against unlawful access or further processing of the data by third parties. This is inherent to the finality principle. If the publication is intended for a restricted target group, such as the members of a sports club, access must also be actively restricted to that target group. In addition to general blocking of personal data from search engines, the controller must only enable access specifically to the target group described in the purpose. In many cases, this can be achieved by means of a password, provided these are publications that do not contain sensitive data or data which in some other way carry major risks for the data subjects. Controllers must also work with individual passwords or access codes, rather than with generic passwords. In order to further reduce the risk of unauthorised access, the passwords or access codes must have a limited period of validity, must be sufficiently 'robust' and must be stored with the controller in an encrypted form.

If, however, the publications incorporate sensitive data, such as medical records or criminal data, the combination of login name and password is too weak. In such cases, the controller must seek other appropriate technical measures to guarantee that only those persons who are authorised to do so can gain access to specific personal data.

WEBSITE INCORPORATING MEDICAL RECORDS

In late 2000, the Registratiekamer investigated the security of an intermediary website, via which patients can place their medical records on the Internet.[78] The website enables patients to monitor their medical data and have it checked by their doctor or pharmacist in an online environment. Doctors, pharmacists and other care providers can also add data to the records, with the consent of the patient. The company that is responsible for the data processing manages the passwords for the log-in procedure of the patients and care providers. To begin with, the Registratiekamer stated that the processing of patients' medical data via the Internet carries risks. In the opinion of the Registratiekamer, the combination of security measures taken by the company was, in view of the current status of technology and in view of what could reasonably be required of the company, satisfactory for the time being. The company had chosen not to include the name and address details of patients in the electronic records. In addition, both communications via the Internet and access to the database were and are encrypted with a 128-bit key and records are frozen after three incorrect log-in attempts. The Registratiekamer felt, however, that the use of a log-in name and password as a form of access security for the records on the site formed a weak link in the security.

The Registratiekamer wrote: *Access security by means of a log-in name and password is generally considered to be too low a level of security.* Depending on the development of technology and acceptance by citizens, the Registratiekamer saw two alternatives for the future: use of biometric access security or use of a so-called challenge-response token card, a system like the one used for home banking. Pending this development, the Registratiekamer recommended that the log-in procedure be tightened. Following the allocation of a new or amended password, the patient would have to be obliged to choose a personal password the first time he or she attempted to log in.

77) LJN: AZ8818, Judge in interlocutory proceedings of Dordrecht District Court, 68382 / KG ZA 07-25

78) Registratiekamer, z2000-00926, 20 June 2001, http://www.cbpweb.nl/documenten/uit_z2000-0926.stm. The site is still in existence and continues to make use of password protection.

8.4.1 Dictionary attacks

The reason that the combination of log-in name and password is considered weak lies in the possibility of authorised users themselves passing on the combination to third parties (also, in some cases, unconsciously, due to spyware on the user's computer), but also in so-called dictionary attacks. Passwords are generally stored in an encrypted format, but specialised software exists that fires an infinite number of log-in attempts at servers. Some programmes can try out several hundred millions of passwords per second. The work of the attackers is made easier by the fact that, in practice, the average password is too weak. According to the renowned security expert Bruce Schneier, almost a quarter of all passwords can be guessed with just 100,000 combinations (based on a list of one thousand words, each accompanied by a hundred frequently occurring suffixes).[79)]

8.5 Security of data transfer

In principle, data transfer across the Internet takes place via open connections. Controllers must ensure that the collection of personal data via websites is carried out securely, for example using an https connection. The use of a connection secured by means of the SSL protocol[80)] entails barely any costs and the deployment of such a connection protects the transfer across network hubs. An unsecured site gives rise to the risk that third parties, for whom the entered data are not intended, intercept the data, for example by taking over sessions or by means of data theft at Internet hubs.

The application of a SSL certificate is also important for authentication of the website itself, in order to reduce the risk of 'phishing'. Sites that are unsecured can be imitated more easily by sites with similar domain names. By imitating these websites, third parties can gain possession of personal data fraudulently.

DIGIDOOR

In 2005, the Dutch DPA carried out an investigation into Digidoor, an initiative of primary schools in the municipality of Almere to publish students' data on the Internet.[81)] In Digidoor (an abbreviation of 'Digitaal doorstromen', which is Dutch for 'Digital transfer'), data relating to primary school pupils are collected for the purpose of facilitating enrolment in secondary education by means of data transfer. The files contain a great deal of sensitive information relating to pupils, such as comments regarding the level of the pupil's numeracy, language and reading skills, but also information regarding fear of failure, concentration issues, health problems and, in exceptional cases, problems relating to the student's home environment. The website was accessible via the Internet without further encryption, as the level of security required was not considered thoroughly beforehand. Following negative publicity, the responsible schools swiftly took a number of specific measures:

– The installation of a dedicated server and an encrypted SSL connection.
– The definition of the various roles for entering and viewing the information and for establishing the retention period for (identifying) data.
– The compilation of a brochure, comprising a further explanation of the technology, content and operation of the system.

The problems could have been prevented if a thorough security plan, including a threat analysis, had been drawn up in advance.

8.6 Protection of machines against unauthorised access

Both well-known and obscure websites frequently appear in a negative light in the news, because their security is insufficient and personal data become accessible that are not intended for publication. This may be the case, for example, if the URLs generated following a log-in procedure follow a predictable pattern. In that instance, third parties can easily 'guess' different URLs and thereby acquire access to the personal information of data subjects. The security and design of the server(s) on which the data are stored therefore form a separate point of concern. The controller must ensure that the machines are protected against unauthorised access by third parties, by consistently following up on security advice. This applies to both the operating system and the software that runs on a server. It is advisable to establish a strict separation between the database in which the data are processed and the server by means of which data are published on the Internet, most certainly when the data being processed are sensitive data. The risks involved in the publication of sensitive data warrant that data being sent from

79) The Washington Times, 'Chances are your password is at risk', 20 January 2007.
80) Secure Sockets Layer (SSL) is a standard protocol that makes use of 'public key encryption' technology to provide a secure service between Internet servers, in which the privacy of the communication, the integrity of the communication and the verification and/or the identification of the sender/recipient are all safeguarded.
81) Dutch DPA, 27 May 2005, z2004-1152, URL: http://www.cbpweb.nl/documenten/uit_z2004-1152.shtml

the database to the server may only be sent in an encrypted format and can only be decrypted at client level.

ACCESS TO DIGITAL ANNUAL STATEMENT

In March 2007, it emerged that the digital annual financial statements of the Uitvoeringsinstituut Werknemersverzekeringen (UWV) [a body implementing employee insurance schemes] had accidentally become accessible to other clients, if two people logged in at the same time. Questions were posed in the Lower Chamber with regard to the incident.[82)]
The UWV informed the Minister of Justice and the Dutch DPA that electronic access had been terminated within one hour of the fault being detected. Each person who accidentally viewed another person's statement was contacted by telephone.

FOLLOWING PUBLICATION

9 Deletion of unlawful data

Even after the publication has appeared on the Internet, controllers must strive to ensure continued compliance with the Wbp. A publication that was lawful because a data subject gave his or her consent, becomes unlawful the moment that the data subject withdraws his or her consent (see Chapter II, section 4.1.) Personal data that were accurate at the time of publication may become incorrect in the course of time and may therefore convey an incomplete representation (such as: X is furious with Y, whereas X may have made up with Y a long time ago).

Owners of websites or forums are also accountable under the Wbp for the publication of incorrect or unnecessary personal data by visitors to their publication. The controller must therefore ensure active moderation in order to prevent the publication of data that is evidently unlawful, most certainly if the data are sensitive, such as criminal data or data relating to health (see chapter I, section 8). In order to prevent the publication from becoming unlawful, controllers must ensure that contributions can only be published at times when moderators are available.

9.1 Obligation to delete incorrect data

In some discussion forums, separate discussion topics (or threads) are opened with regard to reports that, upon closer inspection, have turned out to be incorrect, for example in the case of accusations of spam, fraud or other criminal offences. The original communications containing incorrect personal data then remain available via the Internet. Being able to add another view (rather than delete or correct personal data) is a practice that applies in some instances in the case of archives that fall within the scope of the Archiefwet [Public Records Act]. The purpose of preserving (a part of) Dutch cultural heritage makes it possible to retain archive records in archive depositories for an indefinite period, even if they contain data that are patently incorrect. Article 36, paragraph four of the Wbp makes a similar method of operation possible for data carriers in which amendments cannot be made, such as CD-ROMs or microfiches.[83)] These exemptions do not however apply to (non-journalistic) publications on the Internet. The Wbp does not offer controllers of Internet publications any scope to limit themselves to maintaining a separate list of data that are evidently incorrect. If the personal data stated in a contribution are factually incorrect or excessive in respect of the purpose stated, the publication is unlawful and the contribution must be deleted.

82) Parliamentary Documents II, 16 April 2007, UB/S/2007/12116, responses to question of Members of Parliament Van Hijum and Omtzigt (CDA).

83) Article 36, paragraph 4 of the Wbp: 'In the event that the personal data have been recorded on a data carrier that does not permit amendments to be made, the controller must take the necessary measures to inform the user of the data that the data cannot be corrected, nor supplemented, deleted or blocked, despite the fact that there are grounds for the data to be amended on the basis of this Article.'

ACCUSATION OF FRAUD

In a discussion forum on the subject of fraud, Ms X is accused by Mr Y of sending a brick instead of the digital camera that was promised. Ms X is mentioned by name, including her alleged address, bank account number, IP address and references to other accusations. Ms X appears, however, to have been confused with another person with the same surname and initial. She wants all postings in relation to her to be deleted immediately from the forum. Is Mr Y therefore liable for the comment and must Ms X therefore approach Mr Y for the postings to be corrected or deleted? The answer is no. Under the terms of the Wbp, the owner of the forum is responsible for the personal data on the forum. In this instance, Ms X can approach the forum administrator to have her personal data corrected or deleted. The forum administrator can only refuse such a request if he or she can demonstrate that the publication serves a greater purpose than Ms X's right to the protection of her privacy, for example, because he or she can demonstrate that Ms X has not been confused with another person. The forum administrator is not permitted to refuse the request by making reference to a provision in the general terms and conditions that states that contributions are not deleted under any circumstances. A general provision of this type contravenes the Wbp, because there is no underlying consideration of interests. The administrator is also not permitted to limit him or herself to appending Ms X's reply to the current discussion.

III

DATA SUBJECTS' RIGHTS

1 Introduction

Data subjects, the natural persons with regard to whom personal data are published, may be drastically harmed by incorrect, incomplete or unnecessary publication of their personal data. Inaccurate conclusions can be easily drawn on the basis of a single item of data. Superficial representation can cause damage to the way people function, both in their personal lives and within society. Furthermore, the publication of personal data on the Internet can contribute to a data subject becoming the victim of criminal activities, such as swindle and identity fraud. Controllers are obliged to comply with requests made by data subjects in respect of access and requests for the deletion, correction, supplementation, or blocking of personal data in the event that the data are factually incorrect, are incomplete or irrelevant for their purpose, or have been processed in some other way that contravenes a statutory regulation.[84)]

2 Access

In the majority of cases, data processed in publications on the Internet are publicly accessible and free of charge. The data subject therefore does not usually need to submit a formal request to the controller in order to gain access to the data before he or she is able to submit a specific request for deletion or correction. The right of access is of particular importance in the case of publications to which access is restricted. In such cases, a data subject can make use of his or her right of access in order to find out whether data relating to him or her have been included in an access-restricted publication, and if so, which data.
Pursuant to the obligation to provide information as stated in Articles 33 and 34 of the Wbp, controllers must inform the data subjects, prior to publication, of the types of personal data that will be published in relation to them, in addition to the way in which they will be published and the purpose of the processing. The right of access is important, for instance, to controllers that use blacklists. Many discussion forums and popular publications that give visitors the opportunity to respond comprise user regulations with regard to acceptable conduct. Those who repeatedly or severely breach the regulations may end up being placed on a blacklist of blocked IP addresses and/or user names. A data subject then no longer has an insight into the data that are published about him or her.

The data subject has the right to submit an access request, 'freely' (so without stating reasons) and 'at reasonable intervals', to the controller.[85)] The request to inspect the data cannot however be unspecific.[86)] The controller must respond in writing within four weeks. He or she may also reply by electronic means.[87)] In 2003[88)], the Dutch DPA decided that every person, without reservation, has the right to access personal data processed in relation to him or herself. Pursuant to Article 35 of the Wbp, a report must be a complete and clear overview of the data that are being processed in relation to a data subject. This must not be a description or summary of the data, but a complete reproduction. If the report were incomplete, the data subject would of course be insufficiently able to exercise his or her rights under the terms of the Wbp.[89)] In response to very general requests for access, the controller may ask for a more precise request, in order to avoid disproportionate administrative efforts. The controller must furthermore ensure that the identity of the requesting party is thoroughly established (Article 37 Wbp), for example, by requesting a copy of his or her proof of identity, so as to prevent personal data from falling into the wrong hands. The controller may ask for a maximum of € 0.23 per page for an access request, up to a maximum of € 4.50.[90)] This fee must be paid back if, following access to the publication, the controller must honour a request for correction, deletion, supplementation or blocking of the data.

84) For a general explanation, see the fact sheet entitled *Data subjects and their rights*. The Dutch DPA also has fact sheets relating specifically to correction and access for both data subjects and controllers. The fact sheets are available on the website of the Dutch DPA, URL: http://www.cbpweb.nl, under 'News and publications', 'Fact sheets'.

85) Article 35, paragraph one of the Wbp

86) Explanatory Memorandum, page 44

87) Parliamentary Documents II, no. 8, page 27

88) Dutch DPA, z2003-01617. URL: http://www.cbpweb.nl/documenten/med_uit_z2003-1617.shtml

89) This interpretation was confirmed in mid-2007 by the Supreme Court in the judgments on the Dexia case, Supreme Court, 29 June 2007, LJN: AZ4663 and Supreme Court, 29 June 2007, LJN: AZ4664.

90) Article 39 of the Wbp and the corresponding Besluit Kostenvergoeding rechten betrokkene Wbp [Data subjects rights Reimbursement Decree with the Wbp] of 13 June 2001.

3 Correction and deletion

Data subjects have a far-reaching right to correction. Pursuant to Article 36 of the Wbp, they may ask controllers to rectify, supplement, delete or block data in the event that they are factually incorrect, or are incomplete or irrelevant for their purpose, or have been published in some other way that contravenes a statutory regulation. Should they refuse to correct data, controllers must give reasons for doing so.

When dealing with requests for correction, it makes a difference on which legitimate ground the publication is founded. Data subjects who have given their consent to publication (Article 8, paragraph a of the Wbp) can always withdraw their consent (see chapter II, section 4.1.1). In such cases, sites must always comply with a request for deletion and take this possibility into account beforehand in the technical design of their systems. If the publication is based on one of the other legitimate grounds for publication specified in Article 8 of the Wbp, a data subject may request that data be deleted or corrected in the event that the data are factually incorrect, incomplete or irrelevant for their purpose, or have been published in some other way that contravenes a statutory regulation. If the request is justified, the controller is obliged to comply.

USER GENERATED CONTENT

Nowadays, almost everyone who has a mobile phone is able to take photos and record short films. Recording these types of short films of each other and posting these on the Internet is particularly popular. Profile sites and special user generated content services subsequently make it possible for anyone to access this content, without making it easy to trace the individual who originally posted the information.

The providers of services involving user generated content can in principle be regarded as being jointly responsible for the processing of personal data on their service on the Web. The publication in the absence of legitimate grounds of imagery of natural persons that constitutes an invasion of the subject's privacy can have particularly far-reaching consequences for the data subject(s) and is in any event contrary to the Wbp. If an individual wishes to have the information deleted, he or she should, in the first instance, approach the person who posted the information. If this is not possible or does not resolve the problem, the individual may inform the service provider that the material in question is unlawful. The information must be deleted in the event of obvious unlawful publication pursuant to the Wbp. (See also the explanation in section I.2.)

4 Right to object

In addition to the right to correction and deletion, the Wbp also grants data subjects the right to object. This right only applies if the publication is justified by a legitimate ground as stated under Article 8, paragraph e or f of the Wbp (the effective fulfilment of a task under public law or the result of an individual consideration of interests). Over and above the stipulations of Article 36 of the Wbp, a data subject may in such cases lodge an objection to the publication in accordance with Article 40 of the Wbp, by pleading specific personal circumstances. This 'right to object' relates to publications that are, in themselves, lawful, but which, by virtue of the data subject's special circumstances, may be unlawful in relation to the data subject. In the event that a data subject lodges an objection, the controller must make a new, specific comparative assessment of his or her own (justified) interests and the interests of the data subject. Should the data subject disagree with the outcome of that revised comparative assessment, he or she may apply to the court for a judgment.

Model declaration for the data subject's right of access and right to correction[91)]
A controller of an access-restricted website containing data on non-payment in a specific sector can inform data subjects of their right of access and their right to correction by means of a privacy statement. In accordance with the obligation to provide information, as stated in Articles 33 and 34 of the Wbp, the data subjects must first be informed of the purpose of the blacklist, the identity of the controller and the duration and consequences of being placed on the blacklist before their data are placed on the website. The publication is justified under Article 8, paragraph f of the Wbp, in order to uphold the legiti-

91) This model declaration is suitable for private individuals and companies that justify the publication using the ground for publication stated under Article 8, paragraph f of the Wbp, the consideration of the legitimate interests of the controller in relation to the data subject's right to the protection of his or her privacy. In this instance, both the right to object, expressed in Article 40 of the Wbp, and the right of access and the right to correction or deletion, expressed in Article 36 of the Wbp, apply.

mate interests of a specific category of companies to possess some information with regard to the payment history of a potential client, before proceeding to issue credit. Data subjects can choose whether they wish to have incorrect data corrected by pleading Article 36 of the Wbp, or whether they wish to invoke their right to object, as stipulated in Article 40 of the Wbp. The latter may be the case if the data subject has specific personal circumstances, as a result of which he or she will be disproportionately harmed through inclusion in the blacklist, even if the data are in themselves correct.

A declaration with regard to a data subject's right of access and right to correction may have the following format:

- Access to a restricted section of the website

Should you wish to view your personal data on the restricted section of the website, you may submit a request to that end by sending an e-mail to the following address: privacy@<name website>.nl. You will receive a reply, free of charge, within 7 working days to inform you whether your data are (still) being processed, with what purpose they are being processed and to inform you of the duration of the processing. You may also request a detailed report of all data relating to yourself. Such requests will be complied with within four weeks. The costs of this will be up to a maximum of € 4.50, depending on the quantity of data.

- Right to object

If you are of the opinion that the processing of your personal data violates the protection of your privacy in connection with your specific personal circumstances, you may report this to the following e-mail address: privacy@<website name>.nl. If your objection is justified, your data will be deleted. No costs are associated with such requests.[92)]

5 Exemption: public registers

Public registers introduced by law form an important exception to the rule that data subjects have authority over the publication of their personal data. The underlying reason for public registers such as the Commercial Register or the Land Register is that they are introduced by law to serve a specific public interest. In relation to public registers, data subjects are not given the opportunity to lodge an objection or request deletion by making an appeal under the Wbp, even if the registers are published on the Internet. In the case of public registers, the data subject's rights depend on the rights granted to them by the specific act.[93)] Due to the lack of a general facility to have excessive data removed, it is extremely important that the government continues to make an express distinction, when publishing public registers on the Internet, between the data that are necessary to obtain a service from the government (such as a permit) and data that are published on the Internet. In its recommendation of 15 May 2007 regarding the Wet algemene bepalingen omgevingsrecht (Wabo)[94)] [an Act relating to the general stipulations of environmental law], the Dutch DPA wrote: *It is necessary to reflect upon the issue of why publication would automatically include publication on the Internet. Personal data that are published via the Internet can be collected and processed by an unknown number of Internet users from across the world for their own purposes, even years after the original publication has disappeared from the Internet. The benefit of digitisation must not result in a situation in which personal data are outlawed via the Internet.*

92) In accordance with Article 40, paragraph three of the Wbp, controllers may request a fee of no more than € 4.50 for dealing with an objection, as specified in the Besluit kostenvergoedingen rechten betrokkenen Wbp (13 June 2001, Bulletin of Acts, Orders and Decrees 2001, 305). The fee is paid back in the event that the objection is deemed to be justified.

93) Article 36, paragraph five of the Wbp specifies that the right to correction and deletion does not apply to public registers that have been introduced by law, in the event that the law already includes a procedure for correction, supplementation, deletion or blocking of data. The right to object, as specified in Article 40 of the Wbp, does not apply in any respect to public registers that have been introduced by law, regardless of whether the Act does or does not comprise a special procedure.

94) Dutch DPA, letter to the members of the standing parliamentary committee for VROM [Ministry of Housing, Spatial Planning and the Environment], z2007-00304, 15 May 2007, http:www.cbpweb.nl/documenten/med_20070515_wabo

IV

APPLICABILITY OF EXEMPTION FOR THE PURPOSES OF JOURNALISM

1 Introduction

The Wbp only partially applies to the processing of personal data for exclusively journalistic, artistic or literary purposes. Only the exemption for the purposes of journalism is discussed in further detail in these Guidelines, in view of the fact that appeals are seldom made for an exemption for artistic or literary purposes.

The following do not apply:
- The obligation to provide information (Articles 33 and 34 of the Wbp)
- The prohibition on the processing of sensitive data (Articles 17 to 23 inclusive of the Wbp)
- The notification obligation (Articles 27 to 30 inclusive of the Wbp)
- The data subjects' rights (Articles 35 to 42 inclusive of the Wbp)
- Supervision by the Dutch DPA (Articles 51 to 75 inclusive of the Wbp)
- The restrictions in relation to transfer (Articles 76 to 78 inclusive of the Wbp).

The following, however, do apply:
- The definitions and scope of the Wbp, including the provision with regard to minors (Articles 1 to 5 inclusive of the Wbp)
- The obligation to exercise due care and attention when processing data (Article 6 of the Wbp)
- The obligation to collect personal data for well-defined and legitimate purposes (Article 7 of the Wbp)
- The obligation to have a reason that makes processing data legitimate (Article 8 of the Wbp)
- The prohibition on incompatible use (Article 9 of the Wbp)
- The prohibition on retaining data in an identifying format for a longer period than is necessary (Article 10 of the Wbp)
- The prohibition on processing excessive, irrelevant personal data (Article 11 of the Wbp)
- The obligation to take appropriate security measures (Article 13 of the Wbp)
- The provisions relating to the relationship between the controller and the data processor (Article 14 of the Wbp), to the testing of codes of conduct by the Dutch DPA (Article 25 of the Wbp) and to compensation (Article 49 of the Wbp).

Article 3 of the Wbp is based on Article 9 of the general European Privacy Directive. The Directive has made exemptions for the media mandatory, but 'only in so far as these prove necessary'. That means that Member States may only provide exemptions in so far as they prove necessary in order to find a balance between the protection of privacy and the protection of freedom of expression. For that reason, journalistic publications are not exempt from the general requirements in relation to due care and attention that are stipulated in the Wbp, nor the obligation to take measures to guarantee the security of the data processing.

2 Definition of exemption for the purposes of journalism

In what instances is a publication on the Internet eligible for the exemption for the purposes of journalism and in what instances is that impossible? Establishing the boundary between journalistic and non-journalistic publications is hugely important in order to determine when the Dutch DPA can act as an enforcement body and when other forums are authorised to take action, such as the Courts and the Raad voor de Journalistiek [Press Council in the Netherlands].

3 Criteria for the purpose of assessing whether the exemption applies

The publication of personal data on the Internet falls under the exemption for the purposes of journalism if the publication is in the interests of society and has been produced in a journalistic capacity (and therefore not necessarily by a journalist). Whether a publication serves an exclusively journalistic purpose for good reasons, must be assessed by viewing the publication in its context and then considering the various interests involved. When assessing publications, the Dutch DPA applies the following criteria:

a Is the activity oriented towards (objective) collection and distribution of information?
b Is it a regular activity?
c Is the aim of the publication to raise a topic of social significance?
d Does the publication grant data subjects the right to reply or obtain rectification after publication?

The exemption for the purposes of journalism certainly applies in the event that a publication satisfies all four of the criteria.

3.1 Objective collection of information

Is the publication oriented towards essentially objective collection and distribution of information? It is not only the publication itself that counts in relation to this criterion, but also the nature of the responses, if it is an interactive publication. In order to be eligible for the exemption for the purposes of journalism, it is important that a distinction is drawn between facts, claims and opinions, as the Raad voor de Journalistiek also specifies in its Guideline.[95] Whether a discussion forum or a publication that provides visitors with an opportunity to respond can make an appeal for exemption for the purposes of journalism, partly depends upon the quality with regard to how visitors' replies are moderated. Can visitors to the website freely submit contributions that are clearly harmful to third parties, or are the replies screened?

3.2 Regular activity

The issue of whether a publicist is paid for his or her publication is not an essential factor when determining the scope of the exemption for the purposes of journalism. Only a few people have the privilege of being able to earn money with an (independent) publication on the Internet, while the publication may very well serve a substantial public interest. An assessment is made of whether it relates to a regular activity. A weblog with a couple of outdated contributions would have more difficulty relying on the exemption for the purposes of journalism than a publication in which new contributions are published on a regular basis.

3.3 Social significance

Free debate of social topics is in the public interest. Publications by activists or interest groups in which personal data are processed may be of significant value for revealing criminal acts and misconduct, for the protection of public safety and health and for preventing the deception of the public by actions and publications by persons or organisations. This does not however mean that all Internet publications comprising personal data of this type serve an exclusively journalistic purpose.

Whether the processing of personal data for a publication is indeed exclusively for the purposes of journalism partly depends upon the other three assessment criteria and the capacity of the persons whose personal data are being published. If, for example, a publication reveals incidents of misconduct by a member of parliament or by the director of a well-known or large company and the publication is based on sufficient documentation for it to be credible, the publication of course serves a general social interest. If, on the other hand, a publication exposes the private life of an unknown person, whose conduct exerts no influence upon the way in which society functions, it would be difficult to assert that the publication serves the public interest.

3.4 Right to reply

Finally, in order to be eligible for the exemption for the purposes of journalism, there must be a right to reply.[96] That right means that data subjects have the right to reply or obtain rectification of incorrect information after publication, justified because the right of access and the right to correction do not apply to publications that exclusively serve the purposes of journalism.

Following the Recommandation of the Council of Europe, every data subject has the right to react (free of charge) to incorrect facts concerning him or her in the media, in so far as these facts affect his or her personal rights.[97] The reply must be given a position in the publication that is as prominent as the orig-

95) Guideline of the Press Council in the Netherlands, laid down by the members in April 2007, URL: http://www.rvdj.nl/rvdj-archive/docs/Leidraad_2007.pdf

96) Article 29 Working Party, Recommendation 1/97, Data protection law and the media, 25 February 1997, pages 8-9: 'The directive requires a balance to be struck between two fundamental freedoms.(...) Limits to the right of access and rectification prior to publication could be proportionate only in so far as individuals enjoy the right to reply or obtain rectification of false information after publication.'

97) This is in keeping with Recommendation Rec(2004)161 of the Committee of Ministers of the Council of Europe to member states on the right of reply in the new media environment, URL: https://wcd.coe.int/ViewDoc.jsp?id=802829. 'Any natural or legal person, irrespective of nationality or residence, should be given a right of reply or an equivalent remedy offering a possibility to react to any information in the media presenting inaccurate facts about him or her and which affect his/her personal rights.'

inal statement. Following the recommendation from the Council of Europe there are some exemptions from the obligation to publish the reply; if the reply is much longer than is necessary, or if the content of the reply is not limited to the correction of the disputed facts. This right also does not apply if the data subject has no valid interest in the reply or if the reply is composed in a different language to the original publication.

When assessing whether a publication falls under the exemption for the purposes of journalism, the controller must place considerable emphasis upon whether there is a right to reply, or whether there is an adequate mechanism in place enabling incorrect, incomplete or excessive data to be corrected or deleted after publication. The right to reply is a low-threshold manifestation of the journalistic standard governing correction[98], which does justice to the interests of not restricting journalistic freedom beforehand by declaring all of the rules of the Wbp applicable.

If, after publication, the data subjects are not given the opportunity to comment on personal data relating to them that are evidently incorrect, the publication cannot be accepted as exclusively serving the purposes of journalism. In that instance, all of the obligations stipulated within the Wbp apply. Controllers of non-journalistic publications cannot satisfy their obligations by adding a comment from a data subject that data are incorrect; they must delete or correct the relevant personal data (see chapter II, section 9.1).

4 Archiving of journalistic publications

If the publication falls under the exemption for the purposes of journalism, the publication may also be archived on the Internet, including sensitive data. The exemption for the purposes of journalism continues to apply in further processing operations that take place in libraries and archives, provided that the processing serves a journalistic, artistic or literary purpose.[99] If an archive of journalistic publications is used for other purposes the exemption lapses.[100] When publishing journalistic archives that comprise personal data on the Internet, it is important that a distinction be drawn between the first journalistic interest, i.e. publication and the second interest, i.e. the purpose for which the publications have been archived. The controller must consider for which target group he or she is publishing the archive and the period for which the publication will be available. Regardless of the exemption for the purposes of journalism, the requirements stipulated in the Wbp with regards to non-publication of incorrect or excessive data and with regards to exercising due care and attention, remain in force.

5 Courts and the Raad voor de Journalistiek [Press Council in the Netherlands]

If a publication is subject to the journalistic exemption of the Dutch DPA, the complaint can be dealt with by the judge and in some cases by the Raad voor de Journalistiek. The courts examine whether the publication satisfies the general requirements in respect of due care that are stipulated in the Wbp and tests the publication against the Burgerlijk Wetboek [Netherlands Civil Code].

98) The standard in accordance with the recent guideline published by the Press Council in the Netherlands reads as follows: 'Journalists who appear to have published an incorrect or incomplete communication in respect of an essential point must, as soon as possible and, if possible, on their own initiative, make an appropriate and generous correction that unequivocally clarifies that the communication in the publication or broadcast to be rectified was not correct. In the event that a data subject who, in reasonableness, feels wronged by the communication, replies him or herself, the editors must take the requirement of due care into account when forming the decision as to whether the reply of the data subject will be published, and if so, in what way it will be published.'

99) Explanatory Memorandum, page 73: 'In addition, one must also consider certain data processing operations that take place in libraries and museums. In accordance with the directive, such data processing operations are in line with data processing for the purposes of journalism.'

100) Explanatory Memorandum, page 74: 'The operation of databases implemented on this basis for purposes other than for the purposes of journalism or artistic or literary expression falls outside of the scope of the exemption stipulated in Article 3.'

The general principles of care stated in the Wbp are closely related to the general principles of due diligence as laid down in the doctrine of unlawful acts in the Burgerlijk Wetboek[101] and in case law.[102]

The Raad voor de Journalistiek employs its own criteria for assessing whether a publication serves a journalistic purpose. It considers itself as being authorised only to pass judgment on publications produced by professional journalists, that is to say, people whose chief occupation, whether in employment or self-employed, is to contribute to the editorial direction or editorial composition of publicity media.[103]

From the list of the types of media in respect of which the Raad voor de Journalistiek can pass judgment, it appears that Internet publications may also fall under this category, *in so far as the content of such publications comprises news, reports, dissertations or features that have an informative character.*

Furthermore, the Raad voor de Journalistiek deals with complaints with regard to publications by non journalists if the author is paid for the publication and if he or she collaborates on a regular basis, as is conceivable in the case of contributions of a medical specialist to a professional journal.

101) Article 6:162 of the BW, Section 1. Anyone who commits an unlawful act upon another person, which can be attributed to the perpetrator, is obliged to compensate the other party for the damages that he or she has suffered as a result.
Paragraph 2. An unlawful act is understood to mean the following: the violation of a right, acting in contravention of or failing to act in accordance with a statutory obligation or with that which is considered proper within society under unwritten law, subject to the existence of a justification.
Paragraph 3. An unlawful act can be ascribed to the perpetrator in the event that it can be deemed his or her fault or can be ascribed to a cause that he or she is accountable for by law or by virtue of public opinion.

102) Important jurisprudence on this account is the so called 'Gemeenteraadslid-arrest' [judgement concerning a council member] of the Hoge Raad [Dutch Supreme Court], 24 June 1983, NJ 1984, 801. From this judgement follow seven connected factors enabling the weighing of arguments for the freedom of speech and those regarding the right of privacy. For cases in which these criteria have been applied to publications on the Internet see also: LJN:AO2756, Rechtbank Middelburg, 77/2003, 21 januari 2004, LJN:AT4342, Rechtbank Arnhem, 16 maart 2005 en LJN:AY5772, Rechtbank Zwolle, 122465/KG ZA 06-287, 9 augustus 2006.

103) The Raad voor de Journalistiek [Press Council in the Netherlands] provides a definition of journalistic conduct and journalist in Article 4 of the Articles of Association of the Stichting Raad voor de Journalistiek. 'Journalistic conduct is understood to mean an action or failure to act of a journalist in the practice of his or her profession. Journalistic conduct is also understood to mean, in the context of journalistic activities, an action or failure to act by a person who is not a journalist, but who regularly contributes to the editorial content of the publicity media listed in the following paragraph for a fee.'

V

TRANSFER TO COUNTRIES OUTSIDE OF THE EU

1 Introduction

The transfer of personal data to countries outside of the EU is prohibited, unless one of the statutory exemptions applies. Although Internet publications that are not protected are in principle accessible in countries outside of the EU, this accessibility is not viewed as transfer. In order to overcome the additional risks of accessibility in countries outside of the EU, controllers of publications on the Internet are subject even more so than other controllers to the obligation to exercise due care and attention and to provide data subjects with thorough information on the specific risks associated with the availability of the data outside of the EU.

Only those controllers who explicitly intend to transfer data to a country outside of the EU, as may be the case in a multinational company that operates an intranet comprising personal data, must comply with the regulations relating to transfer.

2 Adequate level of protection

The standard is that a controller is only permitted to transfer personal data to countries outside of the EU if the recipient complies with regulations that offer an adequate level of protection. The decision as to whether a country meets that level is taken by the European Commission or the European Council. Examples of countries that have an adequate level of protection include Argentina, Canada and Switzerland. Specific agreements have been made with the United States with regard to the transfer of information in relation to flight passengers and with regard to the transfer of personal data to companies that have undertaken to apply the Safe Harbour regulations.[104)]

There are a number of exceptions to the general prohibition, for instance, transfer of data is permitted if the data subject has given his or her unequivocal consent or if the transfer is necessary for the performance of an agreement. The Minister of Justice can also, subject to further regulations, grant a specific permit for a transfer or a group of transfers to a country outside of the EU that does not offer an adequate level of protection.

3 Distinction between accessibility and transfer

The Wbp and the Directive do not comprise a separate exemption for the transfer of personal data via publicly accessible Internet pages. According to the letter of the law, the majority of controllers cannot therefore rely on one of the grounds for exemption and the transfer of personal data to inhabitants of the majority of countries outside of the EU is unlawful. In practice, this would lead to impossible situations.

The Dutch DPA therefore follows the line of the Lindqvist judgment of the European Court of Justice[105)] (ECJ), which gives rise to a situation in which the provisions regarding transfer to other countries that do not have an adequate level of protection do not apply, if it is not explicitly the intention of the controller to export the data to such countries.

4 Lindqvist judgment

In late 1998, Mrs Lindqvist, a Swedish citizen, created a number of Internet pages containing information on herself and colleagues in her church parish, including, in some cases, their full names, telephone number, activities and pastimes. Furthermore, she stated that one of her colleagues had injured her foot and was on partial sick leave.

Lindqvist had not informed her colleagues of the existence of the pages or obtained their consent, nor did she notify processing the data to the Swedish supervisory authority. When she was informed that some of her colleagues did not appreciate the pages referred to, she deleted the data relating to them. Nevertheless, the Public Prosecution Department instituted criminal proceedings, based on the use of

104) The European Commission maintains an up-to-date overview of approved countries, URL: http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_en.htm (NB! Including spelling error in URL!)

105) ECJ, 6 November 2003, case C101/01 (Lindqvist)

sensitive data without having legitimate grounds for processing, for failing to notify the data processing and for transferring the data to countries outside of the EU.

The EJC formulated a practical response to the question regarding what the standards meant for transferring data.
'Given, first, the state of development of the Internet at the time Directive 95/46 was drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the Internet, one cannot presume that the Community legislature intended the transfer of data to a third country to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an Internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.'[106)]

The Court also considered that publication on the Internet means that the data are accessible in all countries outside of the EU, whereas the regulation for transfer is intended as a special regulation relating to transfer to a specific country. Since actions 'such as those of Lindqvist' do not constitute transfer, there is no need to investigate whether a person from a country outside of the EU had access to the relevant Internet page or whether the server of this provider is physically located in a country outside of the EU.[107)]

5 International intranet

The Lindqvist judgment is expressly restricted to the case presented, in which the specific conditions are taken into consideration. The ECJ refers to 'action of a person in Mrs Lindqvist's position' and 'actions such as those of Lindqvist'.

If the intention is indeed to make personal data available to a specific group of persons in a country outside of the EU, the standards for transfer do of course apply. That is the case, for example, in a company that has several branches across the world, which makes personal data available to employees in all of the branches by means of an intranet.

6 Due care and attention

Both the French and the British data protection authorities[108)] have followed the practical line of the Lindqvist judgment, yet emphasise that the additional risks of wide publication on the Internet make it even more important that controllers respect all other safeguards stipulated in privacy legislation. The British information commissioner emphasises the obligation to exercise due care and attention. The French supervisory body, CNIL, emphasises the importance of the obligation placed upon controllers of publications to provide information, warning that there is a chance that data could be accessed in countries outside of the EU that do not have an adequate level of protection.

An (additional) duty of care applies in the Netherlands, if the data is to be transferred to countries outside of the EU. In accordance with Article 6 of the Wbp, personal data must always be in keeping with the law and must be processed with due care and attention.[109)] The wording is in keeping with the doctrine of unlawful acts in the Burgerlijk Wetboek.[110)] It relates to due care to be observed in society to prevent an unlawful act. A controller of a publication on the Internet who wishes to exercise due care and attention must specifically take into account the risks of further processing in countries outside of the EU and must adequately inform data subjects that there is a chance that data could be accessed in countries outside of the EU that do not have an adequate level of protection. This applies in particular when the data carry a substantial risk, for example, if they relate to a person's religion or sexual preference.

106) Idem, Consideration 68.
107) Idem, Consideration 70.
108) For the British interpretation, see: The Eighth Data Protection Principle and international data transfers The Information Commissioner's legal analysis and recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbor. Version 2.0, 30 June 2006. For the French interpretation: Délibération n°2005- 276 of 17 November 2005.
109) Processing is understood to mean any action or group of actions in relation to personal data. This may include the collection, recording and organisation of personal data, the disclosure of data to third parties, as well as the copying, retention and destruction of personal data.
110) Article 6: 162 Burgerlijk Wetboek. See footnote 101.

VI

ENFORCEMENT AND THE ROLE OF THE DUTCH DPA

1 Introduction

Controllers that act in violation of the provisions of the Wbp can be subject to civil, administrative and criminal legal action in various manners. Data subjects have a number of opportunities to seek legal redress under the terms of the Wbp, under general administrative law and under civil law. As a supervisory authority, the Dutch DPA also has a number of powers under administrative law to enforce the stipulations of the Wbp.

2 Measures by data subjects

A data subject that believes that his or her personal data are being published unlawfully on the Internet can take action by exercising his or her right of access and right to correction, deletion and to object (see Chapter 3 of these guidelines). Alongside these Guidelines, the Dutch DPA is publishing on www.mijnprivacy.nl specific resources for data subjects, in the form of model letters to controllers and targeted questions and answers on various types of Internet publications.

If the controller does not reply or refuses to comply with a request, a data subject can approach the courts with an appeal to the legal protection offered by the Wbp. In addition, a data subject can submit a claim on the basis of civil law, based on tort for example, or can, for instance, report defamation.

2.1 Legal protection under the Wbp

If a controller does not comply with the provisions of the Wbp, a data subject may request that the courts grant him or her compensation (Article 49 of the Wbp) or that a prohibition be imposed on the further processing of certain personal data (Article 50 of the Wbp).

In a number of specific cases (including in the event that a data subject is refused access to personal data and in the event that a controller refuses to correct, supplement or delete data), the Wbp also offers data subjects the low-threshold facility to submit an appeal to the court, provided that the controller is a company or a citizen. If, however, the controller is an administrative body, the regulations governing objections and appeals from the Algemene wet bestuursrecht (AWB) [General Administrative Law Act] apply.

2.2 Other legal remedies for data subjects

Publications that violate one or more of the provisions of the Wbp are potentially unlawful for other reasons too. In such cases, a data subject has a number of opportunities by which to seek legal redress, in addition to the opportunities offered by the Wbp. A data subject can summon a controller to appear in court on the basis of an unlawful act (Article 6:162 Burgerlijk Wetboek). A data subject can demand that publication be discontinued by means of such a civil proceeding, as well as deletion of data, compensation for material and immaterial damage and reimbursement of legal costs. The data subject can ask the courts to attach an incremental penalty to the judgment.
Other specific legislation may also have been breached, including copyright law, image rights and database law. Another risk for a controller who does not treat personal data with due care is that a data subject can report defamation, libel or other illegal manifestations to the police, such as racist statements, incitement to hatred and publications that violate morality or public order.

3 Enforcement by the Dutch DPA

It is the statutory task of the Dutch DPA to supervise compliance with the Wbp (Article 51 Wbp). The Dutch DPA has a number of tools with which to accomplish this task, varying from mediation to the imposition of incremental penalty payments.

3.1 Mediation, complaints handling and official inquiries

The Dutch DPA can mediate in disputes with regard, for example, to obtaining access to personal data and with regard to correction, supplementation, deletion or blocking of personal data (Article 47 Wbp). The Dutch DPA can also, on the basis of a complaint from a data subject or on its own initiative, institute an inquiry into compliance with the Wbp (Article 60 Wbp).

The Dutch DPA can deploy its powers as supervisory body during such inquiries,[111)] and a controller is obliged to lend its assistance. The Dutch DPA can demand information, demand access to relevant data, investigate cases and resources (including computer equipment), and may enter enclosed spaces, including private residences.[112)]

The number of cases being brought and the complexity of those cases increase continuously however, whilst the remedies available to the Dutch DPA are limited. The Dutch DPA therefore cannot deal with all cases that are brought and, as a result, must decide which cases to select. Regarding complaints, decisions are made on the basis of criteria, such as the seriousness of the breach, how specific the indications are, an assessment of the legal feasibility and the capacity and manpower to be invested by the Dutch DPA, but also particularly on the basis of expectations regarding the potential preventive effect of enforcement in a specific case. [113)]

3.2 Administrative enforcement and incremental penalty payments

In the event of non-compliance with the Wbp, the Dutch DPA can apply administrative enforcement. The term administrative enforcement is understood to refer to an administrative body undertaking concrete action in response to an illegal situation, usually at the expense of the offender. The Dutch DPA can also impose incremental penalty payments. Incremental penalty payments may, for example, mean that a controller must adapt or discontinue a data processing operation under penalty of payment of a specific amount per day. If the controller does not comply with the penalty, the sum of money to be paid can increase substantially to a predetermined maximum amount.

3.3 Criminal enforcement

Finally, a controller also risks criminal sanctions, including sanctions for violating the notification obligation (Articles 27 and 28 in conjunction with Article 75 Wbp).

3.4 International supervision

When investigating violations of the Wbp on the Internet, the Dutch DPA works closely with fellow supervisory authorities from other countries, both within and outside of the EU. The supervisory authorities within the European Union are legally obliged to offer one another assistance and cooperation, in so far as it is necessary in order to conduct investigations into publications on the Internet that they deal with.

111) For all of its supervisory activities, not only in official inquiries.

112) Article 61, paragraph two of the Wbp in conjunction with Article 5:15 Algemene wet bestuursrecht (Awb) [General Administrative Law Act]

113) Vide also the Uitgangspunten en beleidsregels CBP [the Principles and regulations concerning the operation of the Dutch DPA], Government Gazette, 4 October 2004, nr. 190.

MANAGEMENT SUMMARY

Personal data are published on the Internet by government institutions, companies, journalists or individuals in many different ways. Publications on the Internet are generally accessible worldwide, 24 hours per day, to a potentially extensive and highly varied public. The drawback to the benefit of this general accessibility is that people whose personal data are placed on the Internet, the data subjects, could be at a serious disadvantage due to incorrect, incomplete or unnecessary publication of their personal data.

Personal data must be treated with the same care on the Internet as they are offline. This publication by the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] provides clarity with regard to the application of the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act] in cases involving the Internet.

REGULATIONS

In brief, those persons who (wish to) publish personal data on the Internet, the controllers, must adhere to the following regulations.

Prior to publication:

1 Determine whether the publication serves a legitimate purpose and whether that purpose is compatible with the purpose for which the data were originally obtained.
2 Ensure that publication of the data is justified.
The most important justification for publishing personal data is the consent of the data subjects. If obtaining consent is not possible, the controllers must be able to substantiate that publication is permitted on the basis of one of the other five grounds to make data processing legitimate. These are: to carry out an agreement, to comply with a statutory obligation, to safeguard a vital interest of the data subject, to be able to correctly perform a task under public law, or to uphold the legitimate interests of the controller. For each of these five justifications, it is necessary to establish the necessity of publishing the selected personal data on the Internet.
3 Do not publish sensitive personal data.
Special categories of personal data (sensitive data) are data relating to a person's religion or life principles, race, political persuasions, health, sexual orientation, membership of a trade union, personal criminal records and data relating to wrongful or objectionable behaviour. The publication of sensitive data on the Internet is only permitted in the event that the data subject has given his or her express consent or has consciously publicised the data him or herself.

During publication:

4 Observe the obligation to provide information.
Controllers must actively inform the data subjects of the purpose and intention of the publication.
5 Clearly state your own identity, in a manner accessible to each person visiting the publication.
6 Ensure that you do not retain or make available personal data for any longer than is strictly necessary.
7 Actively guarantee the quality and accuracy of the published personal data.
8 Take security measures against unauthorised use.
These measures include data minimisation, protection of personal data from search engines, target group definition and secure transportation of data.

Following publication:

9 Remove data if the data subject withdraws his or her consent to publication.
Comply with requests made by data subjects in respect of access and requests for the deletion, correction, supplementation or blocking of personal data in the event that the data are factually incorrect, incomplete for their purpose or are irrelevant, or have been processed in some other way that contravenes a statutory regulation.
10 Remove wrongfully published personal data. This may particularly apply to publications in which visitors are given the opportunity to respond.

EXCEPTIONS

There are a few exceptions to these regulations for controllers.

1 The first of these relates to using personal data purely for personal or household purposes. The Wbp does not apply to the use of personal data for this purpose. Those who wish to avail themselves of this exception must take security measures to the effect that the personal data are solely accessible to a predefined group of family members, relatives or friends.
2 The Wbp comprises specific regulations for publications with a historic, statistical or scientific purpose. Those who wish to publish personal data on this basis must also strictly delimit access. Moreover, stricter requirements apply in respect of sensitive personal data.
3 The application of the Wbp in respect of publishing personal data exclusively for journalistic purposes is limited.
4 The Wbp includes a prohibition regarding the transfer of personal data to countries outside of the EU, for which an adequate level of protection has not been established. In accordance with the Lindqvist judgment of the European Court of Justice, this prohibition does not apply to publications on the Internet. The fact that publications on the Internet are accessible in various other countries is not regarded as 'transfer'. The regulations apply exclusively to controllers that intentionally transfer personal data to one or more countries outside of the EU, for example by means of an international intranet.

SANCTIONS

Controllers who do not comply with the Wbp can be subject to legal action by data subjects, both on the strength of the Wbp and under administrative law and civil law. In addition, they may be subjected to the supervisory powers of the Dutch DPA, varying from mediation to the institution of an official inquiry or the imposition of incremental penalties.

INDEX OF EXAMPLES

MODEL PRIVACY POLICY

Example privacy policy for a discussion forum

A good privacy policy for a fictitious website with a public discussion forum on an illness may appear as follows: [114)]

1 Identity

The controller for this website is the organisation <name>, Example Street 1, 1000 AB, Haarlem. The organisation can be contacted via info@<name website>.nl

2 Purpose

Via this website and particularly the discussion forum, the organisation wishes to promote the exchange of knowledge in the broadest sense, between both experts and interested parties, in respect of the illness X.

3 Requested information

Registration is compulsory in order to contribute to the discussion forum. Participants are obliged to state their forename and surname, their e-mail address, desired password and their desired pseudonym, under which their contributions will be published. The IP address and time of registration are recorded when registering with the site. The IP address and time are also recorded when publishing each separate contribution. The data obtained on these occasions will not be published on the Internet, with the exception of the chosen pseudonym and the content of the contribution. The organisation uses the non-public data to gain an insight into the types of users of the site so as to enable participants to correct contributions or have them deleted and in order to combat possible abuse, such as spamming, or in order to exclude participants who have breached the user regulations of the forum. The user regulations can be found at http://www.<name website>.nl/userregulations. Furthermore, the e-mail address is used specifically to confirm the chosen pseudonym and password and for issuing new passwords, if necessary. The organisation can also use the e-mail address to forward a message from another participant, provided that the participant has given his or her consent to this at the time of registration. The non-public data are not disclosed to third parties, nor used for any other purpose by the organisation, with the exception of statutory obligations to issue data to competent bodies upon request. If desired, a public profile can be created that is linked to the pseudonym, comprising further information on the person providing the contribution, such as his or her gender and age for example. The creation of a profile is not compulsory.

4 Recipients

The information on the website and in the discussion forum is public and is accessible worldwide. Anyone who contributes to the website thereby agrees that his or her contribution can be reprocessed by an unknown group of readers in an unknown way. In order to avert any adverse consequences of publication, most certainly since this is sensitive data relating to an illness, the foundation deletes contributions in which identifying information pertaining to third parties is published. The organisation strongly advises participants against publishing identifying information about themselves.

5 Participants' rights

By registering with the site, participants in the forum give their unequivocal consent to the organisation to register their personal data and publish their contribution on the Internet, including sensitive data. Minors, that is to say persons under the age of sixteen years, are only permitted to register with

114) With the aid of this example, the Dutch DPA wishes to explain how the ten elements of a privacy declaration can be interpreted in a specific case. The privacy declaration stands separate from any necessary general conditions or specific user regulations. In the context of privacy by design, it is preferable to design systems in which the amount of personal data being processed, if any at all, is limited to the fullest possible extent, and therefore registration of forum participants is not compulsory.

the consent of their parents or legal guardian. All persons are entitled to withdraw their consent at any time and to request that their data be deleted. Upon request, the organisation deletes the data that were necessary for registration and makes the contributions to the forum anonymous. That means that the chosen pseudonym is replaced with the generic term 'deleted' and the corresponding profile, if any, is erased. The contributions themselves remain in the forum, so as not to disturb the logic of the discussion, unless a participant puts forward a special circumstance to have a specific contribution deleted, for example because the contribution identifies the participant.

In order to be able to fulfil a request for deletion or correction, it is necessary that the participant states the data that he or she used to register. The organisation contacts the e-mail address that was given at the time of registration.
The address to which participants must submit requests for deletion or correction is: privacy@<name website>.nl

6 Questions relating to privacy

Questions regarding the privacy policy of the website and forum can be submitted to the organisation by post, to the chair of the board of directors, or by e-mail via privacy@<name website>.nl

7 Other data processing

The website records the IP addresses of visitors to the website, by means of an external statistics programme. That means that all visitors to the website and forum are first routed through an external server, before being redirected to the organisation's website. The statistics are used to measure how easy it is to find the site and to measure usage of (sections of) the site in order to be able to estimate the number of visitors and the necessary server capacity. The website does not make use of cookies or other methods by which to collect data automatically.

8 Security

The organisation uses a protected protocol, https, for the registration of participants in the forum. The data obtained by the organisation in this way are stored in an adequately protected database that is not connected to the Internet. The data on the website and the discussion forum are stored in a database that is linked to the Internet and is adequately protected against unlawful use by third parties, such as amendment of data. All data on the website and in the discussion forum are publicly accessible and can therefore be copied by each third party on his or her own system. The separate pages containing contributions are not indexed for search engines.

9 Retention period

All data on the website and in the discussion forum will remain available on the Internet for as long as the organisation has the resources and facilities necessary for that purpose. In relation to exclusion from the forum, a period of 1 year applies, based on the IP address or IP addresses of a participant that has breached the user regulations. Once the 12-month period has expired, the IP address or IP addresses are deleted from the list of blocked addresses.

10 Notification to the Dutch DPA

The organisation has notified the Dutch DPA of the discussion forum as comprising processing of sensitive data, under number m0000000.

The Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] upholds the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act]. A great deal of personal data is published on the internet. This document provides an indication of how the Dutch DPA generally assesses the publication of personal data on the internet. The guidelines also include an explanation of the Act, illustrated with practical examples.

It is very important that it is clear for everybody who publishes personal data on the Internet whether publication is permitted, in what instances it is permitted and in what format. The intention of these guidelines is to contribute towards achieving this clarity. Transparency in relation to the standards that apply encourages compliance with those standards and is in line with an efficient enforcement policy.

These Guidelines have been published in the Government Gazette on 11 December 2007.

IMPRINT

Dutch DPA Guidelines
Publication of personal data on the internet
College bescherming persoonsgegevens,
The Hague, December 2007.

Postbus 93374
2509 AJ Den Haag
The Netherlands
E-MAIL info@cbpweb.nl

www.cbpweb.nl