THE PROPOSAL FOR A NEW PRIVACY REGULATION: STRICTER OBLIGATIONS AND HEAVY FINES

For many years, most companies doing business in the Netherlands paid little attention to ensuring privacy, i.e. the protection of personal data. The 1989 Personal Data Registration Act had a rather low-key existence. In 2001, it was replaced by the Dutch Data Protection Act (Act),[1] which implemented the 1995 Privacy Directive.[2] However, in the years that followed, privacy seemed to remain an issue addressed mainly by government institutions, the Dutch Data Protection Authority[3] (*College bescherming persoonsgegevens* or CBP) and a handful of legal specialists. In the business community, the Act has often been considered nothing more than an administrative burden, one of the many borne by small and medium-sized enterprises in the Netherlands. The reason for this attitude to privacy was primarily the abstract standards set in the Act. These standards were difficult to implement in concrete terms. The virtual non-existence of sanctions, and the chronic understaffing of the CBP, further contributed to enforcement that was sporadic and focused on excesses.

In the business community, the DPA was often considered an administrative burden.

This business community's attitude started to change when the Dutch Corporate Governance Code[4] effectively resulted in compliance becoming an essential rule of the game for companies operating in the Netherlands. The compliance scorecard included a checkbox for privacy. At around the same time, the commercial use of the internet, including the amount of data collected for commercial purposes, was growing exponentially. Companies such as Google and Facebook took the lead in compiling and exploiting user profiles. This was done by means of cookies (i.e. small text files placed on the computer of a website visitor) usually without the permission or even the awareness of the user. To curb the use of cookies, European regulators introduced the e-Privacy Directive[5] in 2009, thus requiring a company to obtain a user's consent to cookie placement before perusal of the site. OPTA,[6] the Dutch telecoms regulator, was authorised to impose a maximum fine of €450,000 for a violation. In a relatively short time, this new directive reinforced the change in corporate attitude towards privacy. Today most websites of Dutch companies contain extensive information about the cookies used, and they usually expressly or implicitly request the user's consent.

Proposal for a new privacy regulation

Another leap in privacy awareness came with the publication of the European Union's proposal for a new privacy regulation on 25 January 2012.[7] (This is further referred to in this booklet as the "proposed regulation"). This legislation should relieve some aspects of the privacy burden, because it means that in the future an EU business will have only a single set of standards to comply with, rather than the 27 standards of the various member states. However, the proposed regulation also introduces personal data processing rules that are tighter than before and that include heavy fines for a violation. These fines can run up to 2% of the worldwide annual turnover of the company in question. The scope of the proposed regulation includes all companies established in the Netherlands or processing information of Dutch citizens in the context of their business. This implies that many foreign companies which are not established in the Netherlands will have to comply

A further jump in privacy awareness came with the publication of the proposed privacy regulation.

[1] Personal Data Protection Act, Bulletin of Acts and Decrees 2000, 302.

[2] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEC No. L 281 of 23/11/1995 pp. 0031 - 0050.

[3] In Dutch: College Bescherming Persoonsgegevens.

[4] The Dutch Corporate Governance Code - principles of good corporate governance and best practice provisions, Corporate Governance Committee, 9 December 2003. Found at http://www.rijksoverheid.nl/documenten-en-publicaties/richtlijnen/2003/12/09/code-tabaksblat.html (Dutch text).

[5] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJEU No. L337/11 of 18/12/2009.

[6] OPTA is the acronym used in both Dutch and English for the Onafhankelijke Post en Telecom Autoriteit [Post and Telecommunications Authority]. OPTA is charged with enforcement of the Telecommunications Act, which is the act in which the cookie provisions have been included.

[7] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25/01/2012, COM(2012) 11 final.
Found at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

with the proposed regulation and may be subject to supervision by the CBP. Meanwhile, the report on the proposed regulation issued to the European Parliament[8] (called the "Albrecht Report" after its compiler) proposes that even stricter rules may be imposed on the processing of personal data in the European Union. In a number of parliamentary committee discussions on this subject, however, it emerged that a majority of the member states want to weaken some of the provisions of the proposed regulation in order to relieve the burden on small and medium-sized businesses in particular. The European Parliament is expected to vote on the text of the proposed regulation in June 2013. It is therefore expected that in-house legal counsel of companies doing business in the Netherlands will need to monitor these issues in privacy law over the next few months and start implementation in the coming year.

Scope of the proposed regulation

The scope of the proposed regulation has been expanded from that of the e-Privacy Directive. The proposed regulation also applies to the processing of personal data of someone residing in an EU member state if the processing takes place within the framework of the offering of goods or services to data subjects in the EU or the creation of a user profile ("profiling") - even if the processing is done by a controller or processor not located in the European Union.

Consent cannot be used as a basis in employment relationships, given the imbalanced position between the employee and the employer.

Legal basis

As in the e-Privacy Directive, a legal basis for processing personal data will be required. One possible basis is the consent of the individual (sub a). The definition of consent in Article 4:1 of the proposed regulation will make it clear that this consent must be given explicitly each time, either in the form of a statement or a clear affirmative action.[9] Not opting out will no longer be a legal basis for processing personal data. Consent will not be able to form the legal basis for processing if there is a "significant imbalance" between the position of the data subject and the controller.[10] This means that mere consent cannot constitute the legal basis in an employment relationship, given the imbalanced position between the employee and the employer.[11]

Article 6:1(f) will become a common legal basis for processing personal data in the Netherlands. Under this article, processing necessary for the purposes of the legitimate interests pursued by the controller outweighs the protection of the fundamental rights and freedoms (including the privacy) of the data subjects.

What is new is a special provision about the processing of personal data of children (Article 8). To process the personal data of a child below the age of 13, the consent of the child's parent or guardian must be obtained. The controller must make reasonable efforts to verify that the consent was given legitimately.

Heavy fines may be imposed for violations of vaguely formulated obligations.

Article 20 will restrict the collection and further processing of personal data for profiling and the associated marketing.[12] This subject is discussed in more detail in the chapter entitled "Cookies and Consent". This provision will also cover the processing of personal data for job performance reviews and other HR purposes. The legal basis in that case will lie in the employment contract.

General obligations

The proposed regulation will impose several generally formulated obligations on a controller, along with a heavy fine for violations. An example of this is found in Article 11, which will state that a controller is required to have a privacy policy that is "transparent and easily accessible". Information and communications must be provided "in an intelligible form, using clear and plain language, adapted to the data subject." A general obligation to restrict the processing of personal data stems from Article 5(c), which will provide that personal data may be processed for purposes that cannot be fulfilled "by processing information that does not involve personal data." The fact that a heavy fine will be imposed for a violation of such a vaguely formulated obligation is not in accordance with the principle that a criminal offence is only justifiable if clearly formulated.[13]

[8] "Albrecht Report" - Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)).
Found at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

[9] Consideration 25.

[10] Article 7:4 of the Proposed Regulation.

[11] Consideration 34. That was already the prevailing opinion; see Article 29 Working Party, Opinion 15/2011 on the definition of consent, established on 13 July 2011 (WP 187), found at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[12] Profiling is defined as: "… automated processing intended to evaluate certain personal aspects relating to a natural person [data subject] or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour."

[13] See Article 7:1 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and Article 49:1 of the Charter of Fundamental Rights. See also the letter of 11 December 2012 from Dutch State Secretary Teeven, found at http://www.eerstekamer.nl/eu/behandeling/20121211/brief_vande_staatssecretaris_van/document3/f=/vj5dlxksri7s.pdf (in Dutch).

Privacy by design and by default

Article 23, which will provide for "privacy by design and by default", is also formulated in a rather open-ended manner, and will offer companies little guidance for the specific implementation of their obligations. In brief, this provision will require a controller to take measures on the purchase and development of software, the design of databases and, more generally, the setup of an IT system. These measures will have to ensure that the amount of data processed and the associated storage period are in accordance with the goal for which they are collected and also that the data cannot be accessed by an indefinite number of people. These measures will also have to comply with the available level of technology at the time of implementation.

Many company privacy policies will have to be modified to comply with this expanded information obligation.

Duty to provide information

Article 14 addresses the information provided to data subjects. It contains a very detailed elaboration of the information that must be provided to data subjects about the processing of their personal data. What is new is that data subjects must be given clear information about their rights, such as the right to access, rectification and erasure of personal data.[14] Use of profiling and an intention to transfer data to third countries will also have to be specifically stated (see below). Many company privacy policies will have to be modified to comply with this expanded information obligation.

Right to be forgotten

A new right - "the right to be forgotten" - will be introduced in Article 17. This means that, under certain circumstances, the controller will have to ensure that personal data is erased and further dissemination does not occur. This will be the case, for example, if the data subject withdraws his or her consent or objects to the processing, or if the processing "does not comply with this Regulation for other reasons". This last aspect implies that a company must in any case erase the data of its own accord. If the data are erased at the request of the data subject, and these data were made public by or with the consent of the controller, then the controller must take all reasonable measures to inform third parties that processed the data that the data subject has withdrawn his or her consent. Processing of personal data to exercise the right of freedom of expression is excluded from the obligation to erase data.[15] This generally protects the media from the obligation to erase data of individuals at their request.

[14] Article 12 of the proposed regulation.

[15] Article 17:3 makes exceptions to this obligation, among other reasons, for processing for reasons of public interest with respect to public health (paragraph 3(b)); for historical, statistical or scientific research purposes (paragraph 3(c)) or if data must be maintained for purposes of proof (paragraph 4(b)).

Privacy policy

Article 22 will require a controller to have a privacy policy and to implement this in its company. This includes the obligation to store documentation concerning all the processing performed under the controller's responsibility (Article 28), to take suitable technical and organisational measures for the security of personal data (Article 30), to carry out a data protection impact assessment in advance in certain cases (Article 33; see below) and to designate a data protection officer (Article 35).

Under Article 33, companies will have to perform a data protection impact assessment if the processing of personal data poses specific risks to the rights and freedoms of data subjects in view of the nature, scope or purposes of the processing. This will be the case in the following situations: profiling; the processing by the health care system of data relating to a person's sex life, health, race or ethnic origin; the video surveillance of publicly accessible areas; and the processing of large amounts of personal data relating to children or genetic or biometric data.

If a processor violates its obligations, it is subject to the same heavy fines that can be imposed on the controller.

Data protection officer

The appointment of a data protection officer (which in the Netherlands is currently found almost exclusively in government) will be required in all companies with more than 250 employees.[16] The duties of this officer will include the following: supervising the implementation and application of the company's privacy policy and of various provisions of the regulation, such as restricting data processing operations through the application of privacy by design and privacy by default; ensuring the security of data; and complying with data subject requests for information arising from the exercise of such rights based on the regulation. The officer also has an important role in the data breach notification process. (See also the chapter entitled "Data breaches: the introduction of a notification requirement".)

A processor's obligations

Article 26 will impose a number of obligations on a processor, including taking sufficient security measures, acting in accordance with the controller's instructions, and imposing a duty

[16] And smaller companies, if these processing operations require the regular and systematic observation of data subjects due to the operations' nature, scope or purpose. For example, "systematic observation" could apply to headhunters.

of confidentiality on its staff. Under the current legislation, these processor obligations will have to be laid down in a processor contract, and enforcement will therefore be mainly a contractual matter. Under the proposed regulation, if a processor violates its obligations, it will be subject to the same heavy fines as the controller.

Requirement to report a data breach

Articles 30-32 of the proposed regulation will contain a requirement to report data breaches. The basic idea will be that each data breach will have to be reported as quickly as possible to the supervisory authority (in this case, the CBP) and a data subject will also have to be notified in the event of the possibility of negative consequences for the protection of a data subject's personal data or privacy of the data subjects. This is discussed further in the chapter entitled "Data breaches: the introduction of a notification requirement".

Transfer of data to third countries

Another point that will require attention is the transfer of data to a third country, i.e. a country outside the European Economic Area that has not been issued a statement by the European Commission that the country ensures an adequate level of protection.[17] Transfer to these countries will be possible on the basis of binding corporate rules (BCR).[18] These binding rules will apply to all members of the group of companies of which the controller or the processor is a part. Approval by the supervisory authority of a single member state is sufficient for the application of the BCR in all member states. In the absence of BCR, transfer of personal data to third countries will be permitted only subject to the conditions in Article 44 of the proposed regulation, which requires a legitimate ground such as one of the following: consent of the data subject; necessity for the performance of a contract between the data subject and the controller; necessity for the establishment, exercise or defence of legal claims or for the legitimate interests of the controller of the processor if the transfer is not considered frequent or massive. In addition, where necessary, suitable safeguards will have to be offered to protect personal data, taking into account its nature and the purpose and the duration of the processing operations. These safeguards must be documented. As set out in Article 44, for transfer in these cases, a contract will have to be entered into with the party receiving the personal data, and this contract must satisfy the model provisions established by the Commission based on Article 42. With respect to the current regulation on transfer under the e-Privacy Directive, one advantage is that the prior approval of the CBP will no longer be required in the Netherlands. This permit requirement has recently already been eliminated from the Act for cases in which the controller and the receiver have entered into a model contract.[19]

[17] On 1 February 2013, such statements have been issued by the European Commission under Article 41 for Andorra, Argentina, Australia, Canada, Switzerland, Israel, Faroe Islands, Uruguay, Jersey, Guernsey and Isle of Man.

[18] This is under Article 43 of the proposed regulation. These are binding rules that apply to all members of the group of companies to which the controller or processor is a part, and which contain the main obligations arising from the proposed regulation.

Concentration of supervision

For companies located in multiple member states, one major improvement will be that the proposed regulation's enforcement will be the responsibility of the supervisory authority of the member state where the company has its main establishment. This is the location where the company has its central administration in the European Union.[20] This "head supervisory authority" will have to cooperate with the supervisory authorities in the other member states where the company is active. It is possible that the current BCR practice (i.e. a single supervisory authority assesses the rules and approves them and two other supervisory authorities can provide commentary) will be used as a model for the implementation of this requirement.

The maximum fine will amount to 2% of the annual worldwide turnover.

Restrictions and exceptions

Under Article 21, it will be possible for the scope of several provisions (including the duty to inform data subjects about the processing of their data, the right to have data erased and limitations on profiling) to be restricted by national or EU legislation, insofar as this is a necessary and proportional measure in a democratic society. Such a restriction will have to be based on certain grounds, such as the ground that the restriction is necessary to protect the data subject or the rights and freedoms of others. This ground is currently found in article 43 of the Act and may form a basis for suspension of the information obligation when personal data is being processed for a government investigation or in the context of a discovery procedure. (See also the chapter entitled "e-Discovery and privacy: the eternal dilemma?")

Fines

To improve enforcement of privacy rules, the CBP and its European equivalents will be authorised to impose heavy fines after a violation of the proposed regulation. The maximum fine will amounts to 2% of the annual worldwide turnover under Article 79:6 of the proposed regulation).
It will be possible for a fine to be imposed as a result of one of the following:

- non-compliance with requests from a data subject for information on the processing of their data, or for the rectification or erasure of their data (Article 19);

[19] Subparagraph g was added to article 77:1 of the PDPA. Act of 26 January 2012, Bulletin of Acts and Decrees 2012, 33, part K.

[20] Consideration 27.

- incomplete or incorrect documentation of the processing of personal data in the company (Article 28);
- processing of health data and other sensitive data without the required explicit consent from the data subject (Article 9);
- lack of sufficient security measures to prevent a data breach or unauthorised access to or destruction of data (Article 30);
- late or incomplete reporting of a data breach (Article 31 and Article 32); and
- non-performance of a data protection impact assessment on processing operations associated with special privacy risks, such as health data (Article 34).

The Albrecht Report

On 10 January 2013, rapporteur Albrecht, on behalf of the European Parliament's LIBE Committee,[21] which is responsible for this subject, released a report on the proposed regulation. As stated in the introduction, this report supports even stricter rules on the processing of personal data in the European Union.[22] Given the length of this report (over 200 pages) and the limited scope of this booklet, only a few provisions with potentially far-reaching consequences are identified and briefly discussed below.

The Albrecht Report supports even stricter rules on the processing of personal data in the European Union.

One important change recommended in the Albrecht Report concerns the principles for processing personal data.[23] The ground commonly used in the Netherlands is that the processing is necessary for the legitimate interests of the controller and this outweighs the privacy interests of the data subject; however, the recommendation is that this be permitted only in specifically stated circumstances and only if there is no other basis for justification (such as consent). Moreover, the report recommends that the controller be required to inform the data subject about the reasons why the legitimate interest of the controller outweighs the protection of the data subject's privacy.

According to the report, this statement should also be included in the proposal for modifying the information obligations in Article 14, which are further expanded with information about the measures taken in the event of data transfer and about rights and mechanisms to object to or prevent the processing of personal data. Another proposed obligation involves informing data subjects if their personal data is to be communicated to a government agency at its request.

[21] Committee on Civil Liberties, Justice and Home Affairs.

[22] See footnote 8 for the full citation for the Albrecht Report.

[23] Article 6 of the Proposed Regulation.

With regard to profiling, the Albrecht Report proposes only allowing this with the data subject's consent or in accordance with statute.[24] Profiling should be further restricted by excluding the processing of sensitive data and data that make it possible to identify or single out children.[25]

In the Albrecht Report, the proposals concerning the transfer of data to a third country in the context of e-Discovery are subject to stringent conditions.

Another important change proposed in the report is that a company processing personal data relating to more than 500 data subjects be required to designate a data protection officer, even if the company has fewer than 250 employees.[26]

In the Albrecht Report, proposals concerning the transfer of data to a third country in the context of e-Discovery are subject to stringent conditions in the form of a new Article 43a.[27] Any such transfer would only be allowed under a treaty and after authorisation from the supervisory authority. (See also the chapter entitled "e-Discovery and privacy: the eternal dilemma?")

Finally, it is striking that the report proposes that an important enforcement and supervision role be reserved for the European Data Protection Board. This board will be a new agency replacing the Article 29 Working Party. As such this European Union advisory body, in which the supervisory authorities of the 27 EU member states will be represented, will become a privacy "super-authority" that will even have the power to impose implementing rules on a number of subjects.

In the meantime, various parliamentary committees have submitted a large number of proposed amendments. A letter from the Irish EU presidency to the Council recently revealed that a majority of the member states desire the use of a more risk-oriented approach along with, in particular, a reduction in the associated administrative burdens for smaller companies.[28] The next step in the legislative process will be the discussion in the European Parliament, which will then vote (presumably in June 2013) on the text of the proposed regulation. Once the Commission and the Parliament have agreed on the text, the proposed regulation will be submitted to the

[24] Amendment 158, page 102 of the Albrecht Report.

[25] Amendments 162 and 164, pages 104 and 105 of the Albrecht Report.

[26] Amendment 223, page 134 of the Albrecht Report.

[27] Amendment 259, pages 151 and 152 of the Albrecht Report.

[28] Letter of 22 February 2013, found at: http://www.statewatch.org/news/2013/feb/eu-council-dp-regulation-risk-based-approach-public-flexibility-6607-13.pdf.

Council, which will also be the legislative body enacting the new regulation. It is expected that the proposed regulation will come into effect in the course of 2014 or 2015.

The members of the Houthoff Buruma Privacy Team:
Wolter Wefers Bettink
Partner at Houthoff Buruma, Dutch lawyer specialising in IP and IT litigation, privacy and e-business
T +31(20)605 6167 | w.bettink@houthoff.com

Thomas de Weerd
Partner at Houthoff Buruma, Dutch lawyer specialising in IT law, outsourcing, privacy and e-business
T +31(20)605 6985 | t.de.weerd@houthoff.com

Copyright © 2013 Houthoff Buruma

All rights reserved. Short passages from this edition may be used in other publications, under the condition that the source is clearly cited. We prefer the use of the following form: "Privacy: Tips & Tricks for Companies, Houthoff Buruma".

Apart from this, no part of this publication may be reproduced, stored in an automated filing system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of Houthoff Buruma. This publication is provided for informational purposes only and does not constitute legal advice. This publication has been compiled with the utmost care; nevertheless, Houthoff Buruma cannot be held liable for any errors or inaccuracies, nor any associated consequences.