HOUTHOFF BURUMA

PRIVACY

TIPS & TRICKS FOR COMPANIES

2013

IN-HOUSE COUNSEL PRACTICAL GUIDE

This publication is also available as an eBook for iPad.
Using the HB Kiosk App, you can download this eBook and other HB publications free of charge.

HB Kiosk App is available in iPad App Store.

CONTENTS

7 Preface

9 Key points

10 The proposal for a new privacy regulation: stricter obligations and heavy fines

22 Data breaches: the introduction of a notification requirement

32 Whistleblower procedure and privacy

42 Document retention: Data storage and retention periods

50 Cookies and consent

60 Privacy in the cloud

70 e-Discovery and privacy: the eternal dilemma?

82 Sources of European and Dutch privacy law

87 Houthoff Buruma Privacy Team

89 Houthoff Buruma offices

PREFACE

A recent survey of in-house legal counsel in the Netherlands has revealed that privacy, i.e. the protection of personal data, is one of the six themes high on their agendas. This finding contrasts with the business community's general attitude towards privacy in the past following the introduction of both the Personal Data Registration Act in 1989 and the Data Protection Act in 2001. For a long time, most Dutch companies were primarily concerned with the administrative burdens that resulted from the implementation of privacy legislation.

The attitude towards privacy has slowly been changing over the past decade. Awareness of privacy as a corporate issue recently gained significant momentum after the European Commission's publication on 25 January 2012 of its proposal for a new data protection regulation to replace the 1995 Privacy Directive. Although it may take several years for this regulation to be adopted and to take effect - it still being the subject of much discussion - the storm clouds are already gathering on the horizon. The proposed regulation threatens to introduce severe fines for a violation, i.e. up to 2% of a company's worldwide turnover.

This publication is divided into short chapters dealing with seven current privacy-related themes: (1) the new EU regulation, (2) data breaches, (3) whistleblower procedures, (4) cookies, (5) document and data retention, (6) cloud computing and (7) e-Discovery. Many Dutch companies are already dealing with several of these issues, sometimes on a daily basis.

When the proposed EU regulation takes effect, all companies doing business in the Netherlands will have to expend considerable time, effort and money to determine which measures they have to take to protect personal data. Privacy risks will have to be analysed, assessed and described. Adequate security measures, procedures and protocols for the protection of personal data will have to be prepared and implemented. Personal data processing will have to be limited at the source as much as possible. Breaches will have to be reported immediately. Many companies will have to appoint a data protection officer to ensure compliance with the privacy rules.

The challenge facing in-house legal counsel in the Netherlands is to warn their organisations and guide them through the process. We hope that this booklet provides a useful basis and a support for those efforts.

Thomas de Weerd and Wolter Wefers Bettink, partners at Houthoff Buruma, April 2013

KEY POINTS

1. The EU's new privacy regulation will significantly increase the privacy-compliance burden on the business community.
2. Each company will have to develop a plan for dealing with and reporting data breaches.
3. A whistleblower procedure will have to comply with strict requirements to ensure the privacy of the data subjects.
4. A document retention policy reduces expenses and protects against claims.
5. Storing data in the cloud will make it difficult to comply with the new privacy regulation.
6. Complying with the cookie rules begins with figuring out what cookies are necessary.

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

[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).

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.

[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

[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.

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]

[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

[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)).

from the obligation to erase data of individuals at their request.

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

[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.

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]

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.

DATA BREACHES: THE INTRODUCTION OF A NOTIFICATION REQUIREMENT

Data breach means the loss, theft or abuse of personal data.

Data breaches are increasingly in the news. Recent major examples include the hacking incident involving Sony PlayStation Network and Sony Online Entertainment (which affected around 100 million users)[1] and the LinkedIn security breach (where 6.5 million passwords were exposed).[2] In the Netherlands, the publication of the data of 539 KPN customers in early 2012 was cause for panic.[3] The Groene Hart Hospital suffered a security breach involving patient data.[4]

Privacy becomes an issue if a data subject's personal data becomes known outside an organisation. "Stolen" data can be used to perpetrate identity fraud, which could involve something like the purchase of items with stolen credit card details. The company involved may also suffer a loss, because of the cost of investigating the cause of a data breach and dealing with the damage to an affected company's reputation.

The privacy of data subjects comes into play if their personal data becomes known outside the organisation.

At present, only providers of "public electronic communication services" are legally required to report a data breach in the Netherlands. A proposed amendment to the Data Protection Act ("Act") may result in inclusion of a notification requirement for data breaches. The European Commission's proposal for the proposed regulation[5] published on 25 January 2012 also

[1] See, for example, Patrick Seybold, "Update on PlayStation Network/Qriocity Services", Sony's PlayStation Blog, 22 April 2011. Retrieved 26 March 2013 from http://blog.us.playstation.com/2011/04/22/update-on-playstation-network-qriocity-services/.

[2] David Goldman, "More than 6 million LinkedIn passwords stolen", CNN, 7 June 2012. Retrieved 26 March 2013 from http://money.cnn.com/2012/06/06/technology/linkedin-password-hack/index.htm.

[3] Brenno de Winter, "17-jarige bekent hacken KPN", NU.nl, 27 March 2012. Retrieved 26 March 2013 from http://www.nu.nl/internet/2773417/17-jarige-bekent-hacken-kpn.html.

[4] See http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2012/12/06/toezegging-over-informatie-hack-groene-hart-ziekenhuis/lp-v-j-0000002202.pdf.

[5] 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), 25/1/2012, COM(2012) 11 final.
Found at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

includes a notification requirement. Dutch companies are not currently subject to a notification requirement for data breaches, but this does not mean that refraining from reporting a breach is always advisable. In certain circumstances, not reporting a data breach can be characterised as a wrongful act. For example, this would be the case if the data subject has unnecessarily suffered loss or damage. Furthermore, a data breach may itself constitute a criminal act or a wrongful act, e.g. the violation of the medical duty of confidentiality. These points will not be discussed further in this chapter.

Notification requirement for internet and telecom providers

On implementation of the amended 2009 e-Privacy Directive in the Netherlands,[6] a notification requirement for data breaches was included in the new article 11.3a of the Telecommunications Act.[7] The notification requirement, which entered into effect on 5 June 2012, applies primarily to providers of "public electronic communication services".[8] This includes internet service providers (e.g. XS4ALL, Ziggo and UPC) and telecom providers (e.g. KPN, Vodafone and T-Mobile). These providers are obligated to take security measures to protect the personal data and privacy of subscribers and the users of their networks. Article 11.3a of the Telecommunications Act states that a provider must report each breach of these security measures to OPTA if the breach has negative consequences for personal data protection. The subscribers and users affected must be notified if the breach probably has negative consequences for their privacy.

Data subjects must be notified if the breach involves probable negative consequences for their privacy.

In this context, lawmakers have therefore drawn a distinction between (i) breaches expected to have negative consequences for personal data protection and (ii) breaches expected to have negative privacy consequences. In the first situation, only OPTA must be informed; however, in the second situation, both OPTA and the people affected must be informed. In practice, the difference between these two situations seems to be difficult to determine. A safe guiding

[6] 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.

[7] Bulletin of Acts and Decrees 1998, 610.

[8] Act of 10 May 2012 to amend the Telecommunications Act for the implementation of the revised telecommunication guidelines, Bulletin of Acts and Decrees 2012, 235.

principle here is to determine in each individual case whether the data subjects' privacy has been negatively affected or not. The explanatory memorandum[9] to the legislative proposal for the general notification requirement in the Act[10] (described further below) states, for example, that the hacking of the membership records of a sports club might cause an inconvenience but would probably not have negative privacy consequences. However, this would not be the case if the file hacked contained personal data held by the tax department or the organisation responsible for social assistance. Also, notifying data subjects of a breach would not be required if data protection safeguards had been taken to encrypt the personal data concerned, or if another technical method had been used to make these data incomprehensible to unauthorised persons. In this situation, there would also not be negative consequences for the data subjects' privacy.

A notification must describe the nature of the breach. It must also include the contact details of the institution that a data subject can contact in order to get answers to questions and information about the required or optional measures to be taken (such as changing their password or user name). In addition, the provider is required to submit a description of the expected consequences to OPTA, together with information about measures taken or the proposed measures for dealing with the consequences. Providing this information to data subjects is not necessary, because lawmakers have assumed that data subjects do not need to have access to all the information (such as technical data); furthermore, some of the data is confidential in nature. Finally, the provider is required to maintain a summary of all breaches.

The Telecommunications Act gives OPTA the option of imposing a maximum fine of €450,000 if a company violates the obligation to take security measures or if it does not comply with the notification requirement.[11]

OPTA can impose a maximum fine of EUR 450.000 in the case of non-compliance with the notification requirement for electronic communication services.

A company subject to the notification requirement in the Telecommunications Act must report a breach of a security measure as soon as it knows about it. The question that arises is at what point does a company actually have knowledge of a breach: when the IT department discovers it, or only when the management has been apprised of the situation? The answer is

[9] See footnote 11.

[10] Bulletin of Acts and Decrees 2000, 302.

[11] Article 15.4(4) in conjunction with art. 15.1(3), in conjunction with arts. 11.3 and 11.3a of the Telecommunications Act.

presumably that a company must organise things in such a way that, immediately after a data breach is discovered, the breach is reported to the people responsible within the company, after which a decision is taken without delay as to whether the breach should be reported. In certain circumstances, it may be justifiable for a data breach to be "closed" before it is reported, to prevent further abuse as much as possible. On the other hand, the obligation to limit the negative consequences for data subjects as much as possible may mean that it is necessary to report the breach immediately. Because the notification also concerns the amount and type of data exposed to risks, an investigation (of at least some kind) may be necessary before the breach is reported. Of course, such an investigation must be performed quickly and efficiently to comply with the requirement that the notification be made without delay as soon as the company knows about the data breach.

The notification requirement also means that the company concerned has no choice but to independently announce the data breach externally, with all the associated negative publicity and other consequences that will flow from that. It is therefore recommended that a company prepare a communication plan in advance. When reporting, and communicating about, a data breach, the company must make sure that no sensitive business information is disseminated. This must be taken into account in the communication plan.

General notification requirement

A bill to amend the Act is currently awaiting the Council of State's recommendations.[12] Among other things, this bill includes a more general notification requirement for data breaches. This bill is not public at the present time, but an earlier version (i.e. a consultation document) has been published.[13] This earlier version revealed that the amended act will impose a notification requirement on all companies in the public and private sector, with the exception

[12] http://www.rijksoverheid.nl/documenten-en-publicaties/wetsvoorstellen/2012/11/01/wijziging-wet-bescherming-persoonsdata-meldplicht-datalekken.

[13] Amendment to the Data Protection Act and other laws in connection with the expansion of the possibility of using camera images of criminal acts to support law enforcement and the introduction of a notification requirement in the case of breaches to personal data security measures (use of camera images and notification requirement for data breaches) (consultation and advisory version - Dec 2011). Found at http://www.internetconsultatie.nl/camerabeelden. The consultation was closed on 29 February 2012. The amendment proposal for the DPA also contains rules for the use of camera images containing possible criminal acts by private individuals. Camera images with possible criminal acts are subject to the strict regulations of article 22 of the DPA and may be used only to a limited extent. At the request of state secretary Teeven of Security and Justice, additional grounds will be created on the basis of which private individuals and others may use these images to find and identify the parties involved. A large amount of camera images are apparently available, but these are not used sufficiently at the present time. It seems possible that the more efficient use of these images will lead to more of the parties involved being found and identified.

of public electronic communication service providers and financial institutions.[14] Data breach supervision will be concentrated (including for telecommunications and internet providers). The Dutch Data Protection Authority (Authority) will be given the power to levy a maximum fine of €200,000 for non-compliance with the notification requirement.

The CBP can impose a maximum fine of EUR 200,000 in the case of a violation of the general notification requirement for other companies.

Under the new article 34a of the Act, the controller will be obligated to report data breaches to the Authority and the data subjects. In addition, the controller will be required to include in the processor agreement a clause stating that the processor must immediately inform the controller if the processor determines that a security measure for personal data processed for the controller has been breached. For the most part, the requirement in the amended Act will be the same as for the notification requirement in the Telecommunications Act. An important difference will be that a data breach under the proposed article 34a of the Act will have to be reported to the data subjects and the Authority if the breach could result in the loss or wrongful processing of personal data and have negative privacy consequences. As explained above, under the Telecommunications Act, every breach involving personal data must be reported to OPTA, even if there are no expected negative privacy consequences.

Assessment of the breach

Under the Act, an affected company is required to conduct its own assessment of whether the breach could have negative privacy consequences, and must therefore be reported. The criterion for this is whether there is a "reasonable assumption that the breach will lead to a substantial risk of loss or wrongful processing associated with negative consequences for the personal data and the privacy of the data subject". A step-by-step approach is recommended to effectively implement this in practice.

The first step is to determine whether personal data have been exposed to the *risk of loss or wrongful processing*. This assessment must be objective. In practice, it is prudent to assume that this risk exists in principle if a third party has had access to these data without the controller's knowledge. That is the case, for example, if part of an IT system on which personal data are stored has been successfully hacked. This assumption is also justified in the case of loss of an unsecured or inadequately secured flash drive, smartphone or laptop containing personal data.

[14] The rules for ethical business practice in the Financial Supervision Act already contain a security and notification requirement.

Second, it must be determined whether the risk of loss or wrongful processing is *substantial*. This is established by examining the nature and scope of the data breach. As a rule, the risk will be minimal if the loss involves a single device with a limited amount of non-sensitive personal data (such as a smartphone with a list of contacts). However, the risk could be substantial if the member file on a website was hacked.

The third step involves determining whether there are *negative privacy consequences* for the individuals involved. This is based primarily on the nature of the personal data. In the introduction above, the example given was hospital patient data. An incident involving passwords or financial data could also have major negative consequences for the privacy of the data subjects.

A breach involving passwords or financial data could have major negative consequences for the privacy of the data subjects.

The legislative proposal concerning the notification requirement for data breaches includes a fine of up to €200,000 for violations of the notification requirement. In contrast with the Telecommunications Act, a data breach is itself not punishable. In any case, in the light of the present Act, €200,000 is a significant fine; the highest fine currently in the Act is €19,500.[15]

European privacy regulation

Articles 31 and 32 of the proposed regulation also include a notification requirement for data breaches. As in the Telecommunications Act, all breaches involving personal data will have to be reported to the regulator and the data subjects will have to be notified in case there probably are negative privacy consequences.

The proposed regulation imposes a separate requirement on the processor to report a breach of the security measures to the controller. A breach must be reported without unnecessary delay and, if possible, no later than 24 hours after the controller becomes aware of it. A report submitted later than this must include an explanation for the delay. The fine for a wilful or negligent failure to report the breach (or a failure to report it within the specified time or in full) falls under the highest category. In this event, the fine will be up to €1,000,000 or, for a company, up to 2% of its annual worldwide turnover.

Legislative process

At present, it is difficult to predict when a general notification requirement for a data breach will take effect for companies and what the actual requirement will entail. The Dutch bill including a

[15] Article 75.2 of the Dutch Data Protection Act.

notification requirement for data breaches was submitted to the Council of State in 2012. Since the legislative process usually requires at least 24 months, this means it could come into effect at the end of 2014. At that time, the proposed regulation will also have undergone the major part of the legislative process. If the Dutch legislation is ready for enactment more quickly than anticipated, the government will have to decide whether it is useful to put the laws into force at an earlier stage, or whether it makes more sense to wait until the proposed European regulation takes effect.

What is certain is that a general notification requirement for a data breach is on the horizon. In view of the fact that the notification requirement in the proposed regulation is the same as that in article 11.3a of the Telecommunications Act, it would seem to be a good idea for companies in other sectors to start taking steps in this direction.

What is certain is that a general notification requirement for data breaches is on the horizon.

Tips & Tricks

- Take stock of the data processed by the company, with the focus being on sensitive data. What data is being collected, and where?
- Assess the possible risks associated with data loss.
- Maintain a practical but strict policy on the storage of personal data by employees on portable devices, such as laptops, iPads, smartphones and flash drives.
- Ensure adequate security for portable devices used for the storage of personal data (including the option of remotely destroying the data if the device is lost).
- If the company allows its employees to use their own devices for company activities, maintain a strict policy for the personal data stored on these devices and the associated security measures.
- Assess the risks in the IT infrastructure (especially the website and databases) and the decentralised storage of personal data (e.g. peripheral equipment and filing cabinets).
- Prepare a plan of what to do in the event of a data breach. (See below for an example).
- Train the employees involved in the plan.
- Prepare a communication plan for announcing the breach outside the company.

Example of data breach plan

Appoint a "data protection officer" to be responsible for breaches in the company. This person could be the compliance officer, the privacy officer, or an in-house legal counsel.

Appoint a fixed "data breach team" to deal with data breaches. It could include members of the IT staff, the person responsible for privacy, lawyers, and communication experts.

Have the data protection officer and data breach team practise executing the plan on a regular basis.

1. If a data breach is discovered, report it to the data protection officer.

2. The data protection officer immediately informs (1) the data breach team and (2) the responsible director.

3. The data breach team launches an investigation into the incident. The investigation should focus on at least the following aspects:
   a. What type of breach was it (e.g. hacking incident; loss of data; something else)?
   b. When did the breach take place?
   c. What part of the IT system was involved (e.g. website; database; something else)?
   d. What apparatus was involved (if any), and where was this lost or stolen?
   e. What possible data was involved?
   f. What are the actual or expected consequences of the incident?

4. The IT staff on the data breach team identify and carry out measures to repair the breach.

5. Relying on the following factors, the data protection officers and lawyers on the data breach team determine whether the incident must be reported by law, and whether it is considered a criminal act.
   a. Was there a breach of a security measure? (If not, the notification requirement does not apply.)
   b. If yes, were the processed personal data exposed to a substantial risk of loss or wrongful processing?
   c. If yes, will the loss or wrongful processing reasonably lead to negative consequences for the personal data and privacy of the data subjects?

6. If the notification requirement does not apply, the contact person and the lawyers still determine whether it is desirable to report the incident regardless. This decision must take into account the nature and the scope of the breach, the extent to which it involves sensitive data and the possible negative consequences for the data subjects.

7. If the incident must be reported or if reporting is desirable, the contact person draws up the report in consultation with the communications expert and, where necessary, the IT staff and the lawyers in the team.

8. If a criminal act has occurred, such as a hacking incident or data theft, consider whether a report should be filed with the police.

9. If necessary, the communications expert prepares a press release and implements the communication plan.

10. The contact person maintains contact with the regulator about the notification and provides additional information upon request.

11. After the incident has been closed, the data protection officer conducts an evaluation of the execution of the plan of action and the incident itself. Based on the evaluation, possible improvements to the plan of action are made and preventative measures are taken.

WHISTLEBLOWER PROCEDURE AND PRIVACY

"Whistleblower: a person who informs on a person or organisation engaged in an illicit activity." - Oxford

A company or organisation should have an adequate whistleblower procedure for internally reporting suspicions of misconduct within the company or organisation. The importance of this should not be underestimated. The main objective is for management to become aware of dangerous or illegal activities that pose a risk for the company or organisation, its employees, the environment or society as a whole. A whistleblower procedure makes it possible for a company or organisation to take measures in a timely manner to stop misconduct before one of these risks is actually realised. A whistleblower procedure also unmistakeably strengthens a company's corporate governance and can contribute to socially responsible business practice.[1] Finally, a whistleblower procedure, in principle, results in misconduct being reported internally before being communicated externally.[2] It helps protect a company from damage to its reputation.

The importance of a whistleblower procedure should not be underestimated.

[1] The 2011 European Fraud Survey 2011 conducted by Ernst & Young revealed that two thirds of the respondents agree that a company with a strong reputation of ethical behaviour has commercial advantages. Retrieved 26 March 2013 from http://www.ey.com/GL/en/Services/Assurance/Fraud-Investigation---Dispute-Services/European-fraud-survey-2011--recovery--regulation-and-integrity.

[2] See Coen Zoon, Mirjam Stuivenberg, Hans Nauta and Peter Donker van Heel, "Evaluatie zelfregulering klokkenluidesprocedures", ECORYS, Arbeid en Sociaal beleid, Ministry of Social Affairs and Employment, 15 May 2006. Retrieved 26 March 2013 from http://docs.szw.nl/pdf/129/2006/129_2006_3_9270.pdf). (1) Employees working in a company with a whistleblower procedure have a greater tendency to report misconduct in a company (88%) than employees who work In a company without such a procedure (56%). (2) Of those employees who work in a company without whistleblower procedure, 11% tend to report misconduct only externally. If the company has a whistleblower procedure, the employees do not have this tendency. (3) In companies with a whistleblower procedure, there is a strong tendency to report misconduct internally. However, other factors often determine whether misconduct is actually reported, including company culture, the experiences of colleagues, and fear of the consequences of reporting misconduct.

Legal framework

In the Netherlands, the public sector has various whistleblower procedures for civil servants who discover misconduct in their own organisations.[3] However, in the Netherlands there is no specific legislation dealing with whistleblower procedures in the private sector. Legislation does impose certain general requirements relating to such policies, including the Dutch Corporate Governance Code[4] and the Dutch Data Protection Act.[5]

Since the introduction of the 2002 US Sarbanes-Oxley Act (SOX),[6] companies listed on the US stock market can, in principle, be required to create a whistleblower procedure for accounting and auditing issues.[7] This also applies to Dutch companies listed on a US stock exchange, and to Dutch subsidiaries of companies listed on US exchanges. Furthermore, under SOX, a company is prohibited from taking measures against an employee who has cooperated in a whistleblower investigation.[8]

Dutch Corporate Governance Code

In principle, the Dutch Corporate Governance Code (Code) is applicable to companies listed on the Dutch stock exchange. Article II.1.7 of the Code stipulates that these companies must have a whistleblower procedure:

> *The Management Board shall ensure that employees have the possibility of reporting alleged irregularities of a general, operational and financial nature within the company to the Chairman of the Management Board or to an official designated by him, without jeopardising their legal position. Alleged irregularities concerning the functioning of Management Board*

---

[3] See, for example, "Regeling procedure en bescherming bij melding van vermoedens van een misstand" [Regulation on the procedure and protection for reporting suspicions of misconduct], prepared for Dutch provinces and included in the Implementing Regulations of the Collective Employment Conditions Scheme for the Provinces in the Netherlands, version 1 April 2012. Retrieved 26 March 2013 from http://www.adviespuntklokkenluiders.nl/docs/default-source/bibliotheek/regeling-procedure-en-bescherming-bij-melding-van-vermoedens-van-een-misstand-(provincie).xps?sfvrsn=6.

[4] Frijns Code, Decree of 10 December 2009, Bulletin of Acts and Decrees 545. The full text of the Code can be found at http://commissiecorporategovernance.nl/corporate-governance-code.

[5] Bulletin of Acts and Decrees 2000, 302.

[6] Retrieved 26 March 2013 from http://www.sec.gov/about/laws/soa2002.pdf.

[7] Sec. 301 (4) SOX: ("Each audit committee shall establish procedures for (A) the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and (B) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters.")

[8] Sec. 806 SOX.

members shall be reported to the Chairman of the Supervisory Board. The arrangements for whistleblowers shall be posted on the company's website.[9]

The best practice provisions in the Code create a certain standard for the conduct of executive directors, supervisory directors and others. Listed companies are subject to the "comply or explain" principle. This means that companies may depart from Code provisions, but these departures must be explained and justified. Article 2:391(5) of the Dutch Civil Code sets out a company's statutory obligation to state in its annual report that it complied with the provisions of the Code, and to provide an explanation for any departure from a provision.[10]

A whistleblower procedure must comply with the statutory requirements.

Privacy

In 2006, the Dutch Data Protection Authority (Authority) issued an opinion about the use of a whistleblower procedure that took the form of a whistleblower hotline within a multinational company.[11] The Authority and the Article 29 Working Party[12] largely have the same approach, but several additional requirements apply under the Act. (The Article 29 Working Party is the European Commission's advisory body on privacy and has representatives from the 27 EU member states' regulatory bodies.)

Basis

Under article 8 of the Act, there must be a basis for the processing of personal data in the context of a whistleblower procedure. This basis can be a requirement to comply with a legal obligation (article 8(c)) and the company having a justified interest that makes the procedure essential and that outweighs the privacy of the employees involved (article 8(f)).

---

[9] See footnote 4. This Code replaced the Dutch Corporate Governance Code (Tabaksblat Code) with effect from 1 January 2009, decree of 27 December 2004, Bulletin of Acts and Decrees 747, which includes a similar provision.

[10] See also the Decree of 23 December 2004 to establish further rules for the content of the annual report. This decree was amended several times at a later stage.

[11] Dutch Data Protection Authority, Opinion on permit application, by virtue of art. 77.2 of the Data Protection Act, 16 January 2006, 2004-1233.

[12] "Article 29 Working Party, Opinion 1/2006 on the application of EU data protection rules to internal whistleblower procedures in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP117, 1 February 2006" Retrieved 26 March 2013 from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf.

The first basis does not apply if the legal obligation is a foreign one, including for example a SOX obligation. The obligation must be imposed by virtue of a generally binding regulation. The consequences for a controller if it does not comply with a foreign legal obligation (e.g. fines) must also be taken into consideration if the company wishes to rely on "justified interest".

The Authority's position is that a company has a justified interest in having a whistleblower hotline, but this must be balanced with the fundamental rights and freedoms of the data subjects, in particular, the right to privacy.

This will usually support a whistleblower procedure if the intention is to identify substantial misconduct, i.e. presumably entailing a certain degree of seriousness with respect the facts or situations reported. The seriousness will depend on the circumstances of the case. How the misconduct is dealt with must also be proportional: the nature and seriousness of the misconduct affects how the report is made. According to the Authority, the suspicions of a whistle blowing employee must be based on reasonable grounds of possible or actual misconduct.

An organisation is not allowed to encourage the use of anonymous reporting.

The Authority emphasises that a whistle blowing procedure is supplemental in nature, and does not replace the usual methods for dealing with incidents in a company. According to the Authority, passing on such data to a parent company is justified only in a case of substantial misconduct that goes beyond the level at which the subsidiary is operating.

Suspicion of a criminal offence and special personal data

If the report contains information relating to a crime (i.e. a legitimate suspicion of a criminal offence) or special personal data[13] (i.e. concerning a person's religion, philosophy of life, race, political persuasion, health, sexual life or trade union membership), the company must follow a strict set of rules that applies to the processing of special personal data. In reports produced in the context of whistle blowing, this will primarily concern data relating to crime. The company may, in principle, process these data if a staff member has committed, or will imminently commit, a criminal offence.

Anonymous reporting

An organisation is not allowed to encourage the use of anonymous reporting. It must create a system in which it is a basic principle that the identity of the whistleblower is known. The

[13] Art. 16 to 23 of the Dutch Data Protection Act ("Act")

Authority's position is that it is preferable to create a system that allows reports to be made confidentially, i.e. the whistleblower's identity is known but only to a confidential adviser or is kept secret in another way.

Compliance with the duty to inform

The duty to inform entails informing a data subject when his or her data is being processed and also communicating clearly and transparently with staff members about the existence and functioning of the system. In this context, the scope of the system - i.e. which misconduct is to be reported? - deserves special attention. Furthermore, it must be communicated that abuse of the system could lead to the imposition of disciplinary measures. This does not apply to reports submitted by an individual with the best intentions, but that ultimately turn out to be unfounded.

People named in a report must be informed that data concerning them is being processed within the whistle blowing system and this information must be given no later than at the time the data is recorded. In this way, data subjects are given the opportunity to exercise their rights,[14] including the right to access. However, because this could potentially obstruct a criminal investigation, under article 43 of the Act, it is possible to delay informing the data subject as long as necessary for the purpose of securing the evidence. The Authority's position is that this exception must be interpreted restrictively, and use of this exception must be properly substantiated on a case-by-case basis. The right to access may not be used to discern the identity of the whistleblower or the other parties involved.

Accurate, correct and relevant information

The Authority points out that the report must be objective and directly related to the scope of the procedure and that the information may be used only to assess the suspected misconduct. The document states specifically that the report must clearly relate to the suspicion of criminal activity.

Clear and transparent communication must take place with employees about the existence and functioning of the system.

Dealing with reports

According to the Authority, a report must be handled by an outside organisation or, if dealt with internally, by a unit specially designated for that purpose. The preference is to designate an organisation external to the original company or institution to deal with the first report. Access to the reports and the associated data must be limited. Staff members who have access to the

[14] Act, art. 35 to 41

information are subject to a duty of confidentiality. It may be necessary to transfer personal data to a third country; if so, any such transfer must satisfy the requirements imposed by the Authority. For more information, see also the chapter entitled "e-Discovery and privacy: the eternal dilemma".

Dealing with complaints

A standard procedure is required to deal with complaints received through the whistleblower hotline. Particular attention should be paid to the rights of data subjects when dealing with complaints.[15]

Retention period

Data processing in the context of whistle blowing that turns out to be unfounded must cease immediately and the data must be deleted. Data relating to an open investigation may not be stored longer than two months after the investigation is completed, unless disciplinary measures are taken against the whistleblower (i.e. because of a false report) or the subject of the whistle blowing (i.e. because of a legitimate report).

Position of a whistle blowing employee

Under the Works Councils Act,[16] the establishment of a whistleblower procedure requires the approval of the works council. It is often unclear to an employee what his or her position is if the employee suspects misconduct in the company. Moreover, whistleblower cases reveal that an employee who blows the whistle often does so to his or her own detriment.[17] In Dutch employment law, an employer's case against a whistleblower is usually based on article 7:611 of the Dutch Civil Code, which states that an employee is required to conduct himself or herself as a "good employee". (The same standard applies to the employer.) Whether the actions of a whistleblower justify the measures taken by an employer (including, for example, summary dismissal) is a matter to be determined by the court.

Bill for a law protecting whistleblowers

On 14 May 2012, a bill for a whistleblower protection act having the following goal was introduced:

> *...to improve the conditions for reporting social misconduct, by making it possible to investigate misconduct and to better protect people who report misconduct.*

---

[15] Act, art. 35 et seq.

[16] Works Councils Act, art. 27.1(j)

[17] For a summary of the legal precedents, see E.S. de Bock, "For whom the bell tolls, Whistle-blowers in the Netherlands" (2011). Found at http://www.houthoff.com/uploads/tx_hhpublications/Forwhomthebelltolls.pdf. See also HR 26 October 2012, LJN: Netherlands Civil Code 9244.

The bill proposes the establishment of a "Whistleblower Office":

> *The legislation provides for a 'Whistleblower Office' that conducts investigation into social misconduct and makes recommendations to resolve problems. This Office will also provide support and guidance to the whistleblower, if desired. The legislation also provides for a Whistleblower Fund, which provides financial assistance to whistleblowers, if necessary. The Whistleblower Office will become part of the National Ombudsman, but will be open to reports from both the public and private sector. When carrying out its tasks, the Office may seek the assistance of existing organisations and experienced experts. The Office will issue an annual report on its activities. This report will set out the investigations conducted and the outcome of the recommendations.*[18]

The establishment of a whistleblower procedure requires the approval of the works council

At present, it is not clear when the Whistleblower Office will be operational. The Council of State has already issued an opinion. The timeframe will be determined by Royal Decree.

Design of the procedure

Due to the statutory silence on this issue, a company may design its own whistleblower procedure. A good place to start is the 2003 "Statement on dealing with suspicions of misconduct in companies", along with a model procedure prepared by the Dutch Labour Foundation (*Stichting van de Arbeid* or "STAR").[19] STAR notes that it must be clear to employees where they can make a report and what the procedure entails (i.e. what is done with a report and how the employee is informed about the progress of the case).[20] It should also be clearly communicated to employees that this procedure is not intended for employee complaints about personal work issues. Complaint procedures already exist for this purpose. The whistleblower procedure is also not intended to be a means for employees to report ethical dilemmas encountered in the scope of normal business activities. In principle, the whistleblower procedure is also not a forum for employees to criticise the employer's policy choices.

---

[18] *Parliamentary Documents II* 2012/13, 33 258, no. 7, pages 1 and 2.

[19] Statement on dealing with suspicions of misconduct in companies, Dutch Labour Foundation, 24 June 2003, Publication no. 6/03.
Found at http://www.ser.nl/~/media/Files/Internet/persberichten/2004/stvda_nota_20030624.ashx.

[20] Statement (see footnote 19), page 2.

Whistleblower Advisory Point

The Dutch government established an independent agency called the Whistleblower Advisory Point on 1 October 2012.[21] Advising and supporting both potential and actual whistleblowers, the Whistleblower Advisory Point focuses on public sector and private sector misconduct involving society as a whole. If the whistleblower considers the outcome of a company or government organisation's internal report to be unsatisfactory, he may request the Whistleblower Advisory Point to provide a recommendation on an appropriate external organisation where the complaint may be notified (e.g. the relevant supervisory authority). However, it does not actually conduct investigations into misconduct itself. The Whistleblower Advisory Point also provides information to the public about whistleblowing and identifies developments and patterns important for whistleblower policy in the public and private sectors.[22]

Inform data subjects if their personal data is being processed in the context of the procedure.

[21] Established based on the Decision of 27 September 2011 to establish the Committee for the Whistleblower Advisory and Referral Point (Temporary Decision on the Committee for the Whistleblower Advisory and Referral Point) and explanatory memorandum, Bulletin of Acts and Decrees 2011, 427.

[22] See also http://www.adviespuntklokkenluiders.nl.

Tips & Tricks: Preparing a whistleblower procedure

- Prepare the procedure in consultation with the works council or body representing the employees (if any).
- Determine which cases are subject to the procedure.
- Encourage confidential reporting; curb anonymous reporting.
- The procedure should include at least the following elements (but see also STAR's model procedure):
  - the appointment of one or more officers to whom employees can report incidents/suspicions;
  - a description of how the company deals with the internal report;
  - a description of how feedback is given to the person who submitted the report;
  - a description of the situations in which, and the way in which, the whistleblower may make an external report;
  - the protection of the rights of a whistleblower who has acted with due care.
- Inform employees about the existence and functioning of the procedure.
- Inform data subjects if their data is being processed in the context of the procedure.

DOCUMENT RETENTION: DATA STORAGE AND RETENTION PERIODS

Document retention is the storage of company and personal data in accordance with company policy and statutory obligations.

Every company and other organisation must deal with the growing amount of data created and collected by it and its employees. The exponential growth in electronic data has resulted in data storage costs becoming a substantial cost item. There is a need to limit data storage. Can data be destroyed after a certain period of time? This process has various legal aspects that must be taken into account.

Cost reductions can be achieved by limiting data storage without negatively affecting the company's statutory obligations and legal position.

In Dutch law, certain company data is subject to a minimum retention period, whereas personal data is subject to a maximum retention period. In addition, to protect the interests of the company, the validity periods and limitation periods applicable to agreements and compensation claims must, as much as possible, be taken into account when making decisions relating to the retention and destruction of data. Should a dispute arise, the company must have access to all the information needed to defend itself.

Litigation commenced in the United States, or an investigation commenced by a regulator or supervisory body, may involve an unexpectedly far-reaching document discovery process or a mandatory order for the production of documents. (See also the chapter entitled "e-Discovery and privacy: The eternal dilemma".) Because the destruction of data may directly conflict with obligations relating to this, a clear policy for data retention and data destruction is recommended. This helps achieve a reduction in costs relating to data storage, but without negatively affecting a company's ability to comply with its statutory obligations or to defend its legal position in a dispute

General obligation to retain company data

A Dutch legal entity (*rechtspersoon*) is required[1] to maintain records and retain the associated documents and data carriers in such a way that the rights and obligations of the legal entity can

[1] Dutch Civil Code, art. 2:10(1). Article 3:15i states a similar obligation for the self-employed and professional practitioners.

always be ascertained. In addition, information relevant to taxation must always be clear from the records.[2] Relevant documents and data carriers must be retained for a minimum period of seven years.[3]

Dutch law also explicitly identifies a limited number of documents that must be retained, e.g. the balance sheet and profit and loss account of a legal entity.[4] But the law is silent on the other documents that must be retained. It will depend on the type of organisation, but in any case the documents to be retained generally include agreements, permits and licences, staff records, accounting information (including about receivables and debts) and the associated relevant correspondence.

Other specific retention obligations may apply in certain business sectors. For example, the financial sector is subject to an obligation to retain all data obtained in the context of a customer due-diligence investigation for five years after the end of the business relationship[5] and an obligation to retain reports about unusual transactions for at least five years after this was reported.[6]

Maximum retention periods for personal data

If the documents and data retained contain personal data, the Dutch Data Protection Act (Act)[7] is applicable. The Act does not set specific minimum or maximum retention periods, but it does state that personal data cannot be retained longer than necessary for the purposes for which the data are collected or used.[8] The maximum retention period for personal data stated in the proposal published on 25 January 2012 for the EU's new privacy regulation ("proposed regulation")[9] is lower, and the proposal also states that the

Personal data may not be retained longer than necessary for the purposes for which the data are collected or used.

[2] State Taxes Act, art. 52(1).

[3] Dutch Civil Code, art. 2:10(4); State Taxes Act, art. 52(4).

[4] Dutch Civil Code, art. 2:10(2).

[5] Prevention of Money Laundering and Terrorist Financing Act, art. 33; Decree relating to Prudential and Valuation Rules under the Financial Supervision Act, art. 14.

[6] Prevention of Money Laundering and Terrorist Financing Act, art. 34.

[7] Bulletin of Acts and Decrees 2000, 302.

[8] Data Protection Act, art. 10.

[9] 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), 25/1/2012, COM(2012) 11 final. Found at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. ("proposed regulation")

storage period for personal data must be kept to "a strict minimum".[10]

The Act imposes a notification requirement on the processing of personal data. Under a law called the Data Protection Act Exemption Decree (DPAED),[11] exemptions are allowed in certain situations; however, these exemptions are effective only for certain time periods. If personal data is retained for longer than these time periods, the exemption no longer applies and the processing of the personal data must be reported. While these time periods relate to the exemptions, they may also be seen as an indication of the maximum period that lawmakers consider necessary for the retention of personal data in these situations.[12] The table below illustrates the indicative maximum retention periods relating to various types of personal data:

Type of personal data	Notification exemption period / Indication of maximum retention period	Statutory reference
Employee data	2 years after end of employment	DPAED, art. 7:5
Debtors / creditors	2 years after receivable paid	DPAED, art 12:6
Subscriptions	2 years after end of subscription	DPAED, art. 11:5
Job applicants	4 weeks after end of job application procedure, unless permission is obtained for a year	DAPED, art 5:6

Storage method

For the most part, a company may determine how it meets its retention obligations. The documents and data to be stored may be retained in digital form, as long as they are available during the full retention period and can be made legible within a reasonable period of time. Several documents are also subject to an additional requirement that they be retained in paper form, i.e. the balance sheet and profit and loss account.[13]

The Act requires a controller to take suitable technical and organisational measures to secure the personal data against loss or any form of wrongful processing.[14] The proposed regulation

[10] Proposed regulation, consideration 30.

[11] Bulletin of Acts and Decrees 2001, 250.

[12] See also the information sheet published by the Dutch Data Protection Authority entitled "Retention periods for personal data in your hands", dated July 2012. Found at http://www.cbpweb.nl/Pages/inf_va_bewaartermijnen.aspx.

[13] Dutch Civil Code, art. 2:10(4).

[14] Data Protection Act, art. 13.

further elaborates and refines this obligation. Article 23 of the proposed regulation provides that, in determining the processing method and on conducting the process, a controller must implement technical and organisational measures and procedures so that the processing complies with the conditions of the proposed regulation and ensures that a data subject's rights are protected. Furthermore, technical measures must be taken to ensure that the collection or retention of data is limited to the amount and the period strictly necessary in view of the objectives. A company could potentially rely on a document retention policy as one way of carrying out the obligation to implement suitable technical and organisational measures and procedures.

In determining the fine after a security breach resulting from a violation of the proposed regulation, the extent to which the measures required by article 23 were implemented will be taken into account.[15] The lack of an internal policy, or the lack of suitable measures to comply with the proposed regulation (including the article 23 measures), can result in a fine of 2% of the annual worldwide turnover of a company in the case of an intentional or negligent act or omission.[16]

Retention obligations in practice-Document retention policy

Companies and institutions frequently retain many more documents and much more data than strictly necessary, and they do so for a period longer than required by law. Furthermore, the same documents are, in practice, often stored in different locations at the same time. This leads to an unnecessary burden on the company's storage capacity, particularly if a company does not have clear guidelines on what should or should not be stored and if there are no physical or digital limitations on the amount of data stored. Setting a maximum size for mailbox capacity and/or digital archive capacity can be helpful with this.

To make this clearer, a company can introduce a "document retention policy" about retaining and destroying documents. A document retention policy would determine the following for each type of document: (i) how it must be stored, (ii) in what form, (ii) in which physical or digital location and (iv) who is responsible for it. Preparing such a policy document forces a company to actively consider how it wishes to deal with retaining and archiving documents. To limit the costs involved, the company should decide which documents are necessary and relevant, and how long they should be stored.

A document retention policy creates clarity about retaining and destroying documents.

[15] Proposed regulation, art. 79:2.

[16] Proposed regulation, art. 79.6(e).

The following aspects must be taken into account:

1. the statutory retention periods;
2. data storage costs;
3. the need to have access to certain data as evidence in proceedings;
4. the obligation to submit data during a discovery or investigation process.

Providing evidence

Prior to signing a contract, the contract parties frequently have extensive e-mail contact. In some cases, many draft versions of contracts are exchanged. If and when a contract is finalised and signed, the relevance of the preparatory documentation decreases. Still, a situation could potentially arise in which it is useful to have this information, e.g. in a dispute over the interpretation of the contract according to the Haviltex criterion and later legal precedents.[17] If the agreement has expired, and all the obligations in the contract have been satisfied, the preparatory documentation will generally no longer be needed. The decision whether or not to retain such correspondence will involve a consideration of the risks involved in destroying it.

If a company is or may be involved in civil proceedings in the United States, or if the company is under investigation pursuant to regulatory legislation or foreign law, including the US Foreign Corrupt Practices Act (FCPA)[18] or the UK Bribery Act 2010,[19] the company may be required to make available all the relevant information under its control to the other party and/or the regulator. (For more detailed information about this, see also the chapter entitled "e-Discovery and privacy: The eternal dilemma"). If a company has destroyed this information, and there is evidence at that time or later that this information existed, in such civil proceedings the simple fact that the information has been destroyed will in most cases result in losing the case and the imposition of large punitive damages. In the event of regulatory and criminal proceedings, the consequences for the company would be high fines and restrictive measures. However, if relevant data is destroyed in accordance with a document retention policy that is based on objective criteria and consistently applied, this could serve as a legitimate defence on the part of the company.

---

[17] Supreme Court, 13 March 1981, NJ 1981, 635 (Ermes/Haviltex). See also Supreme Court, 19 January 2007, NJ 2007, 575 (Meijer/Pontmeyer).

[18] See "Foreign Corrupt Practices Act: An Overview". Retrieved 27 March 2013 from http://www.justice.gov/criminal/fraud/fcpa/.

[19] See UK *Bribery Act 2010*, 2010 Chapter 23. Retrieved 27 March 2013 from http://www.legislation.gov.uk/ukpga/2010/23.

Introducing a document retention policy

The success of a document retention policy depends on good communications about the intent and implementation of the policy, and its acceptance by the company. It is extremely important to make the employees aware of the importance of the document retention policy and its consistent implementation, both from a risk-control aspect (i.e. retaining the correct documents) and a cost-control aspect (i.e. not retaining documents unnecessarily). It may be helpful to share information with employees about the cost of unnecessary data storage.

The success of a document retention policy depends on good communication and the policy's implementation and acceptance by the company.

A document retention policy should cover not only the decision to retain documents and data, but also the decision to destroy certain documents after time has passed. For documents subject to a maximum statutory retention period, such as documents containing personal data, destruction is mandatory. The company must decide whether to destroy documents after the minimum statutory retention period in the Dutch Civil Code and tax legislation has passed. In the event of a discovery process or a criminal or other investigation, it will be in the company's benefit to be able to demonstrate that the document retention policy was implemented consistently.

Tips & Tricks

- Make a summary of the different types of information stored in the company.
- Determine which minimum or maximum retention periods apply for this information.
- With the approval of the works council or the employee representation body, establish a document retention policy that determines the following for each type of information and document:
  - how long it is to be stored;
  - in what form;
  - at which physical or digital location; and
  - who is responsible for it.
- Communicate the document retention policy internationally to existing and new employees.
- Provide regular information and training to create employee awareness of the policy.
- Distribute a short data retention guide listing the principles that must be observed when purging files and mailboxes.
- To encourage the timely deletion of non-relevant e-mails and data, set a maximum size for the e-mail inbox capacity and/or a maximum length for the retention period for e-mails.
- Ensure that employees store digital documents and other data only on company equipment, and not on their own personal devices.
- If the company permits "BYOD" (Bring Your Own Device), make sure the document retention policy is also implemented on these devices.
- Ensure that employees leaving the company purge their e-mail inbox and, where necessary, provide their colleagues with access to this.
- Inform employees about the costs of data storage.
- Emphasise the importance of using the data retention guide when purging e-mails and data.
- Ensure that stored documents are purged regularly. The need or desire to retain a particular document can decrease over time. Be sure to consider backups as well.
- Have a user panel and the IT department regularly evaluate the document retention policy.

COOKIES AND CONSENT

"Cookies are small text files placed on a computer and accessed by the browser when opening a webpage." - DDMA 2012

The statutory requirements governing the placement of cookies were tightened in the 2009 revision of the e-Privacy Directive.[1] One requirement was an amendment to article 5:3 of the former 2002 e-Privacy Directive,[2] which relates to the placement of information on end devices (such as a computer or a smartphone) and the accessing of information stored on such devices. While the concept of "information" is broader, this provision mainly applies to the placement and accessing of cookies.

Under the former 2002 e-Privacy Directive, it was sufficient to offer the option to refuse cookies (i.e. the opt-out approach). Cookies were placed without the user's knowledge, however, and the user was not given any information about the data being collected. European lawmakers have taken the position that the opt-out approach did not work under these conditions. If a user does not even know that data is being collected, or which data are involved, he or she is not able to opt out. Technological developments, however, have made it possible for companies and institutions to collect and analyse increasingly larger amounts of information and subsequently create individual user profiles on this basis. Since 2002, a market has emerged for behavioural advertising, i.e. providing advertisements based on user profiles.

The requirement for consent and the provision of information apply in principle for all types of cookies.

Under the revised 2009 e-Privacy Directive, the placement and accessing of cookies is allowed only if the subscriber or user concerned has consented to these actions on the basis of clear and complete information. This description is taken from the 1995 Privacy Directive.[3] The consent and information requirement apply in principle for all types of cookies. However, cookies necessary

[1] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337, pages 11 - 36, 18/12/2009, found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:nl:PDF.

[2] Directive 2002/58/EC concerning privacy and electronic communications, OJ L 201 of 31/07/2002, pages 37 – 47, found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:NL:PDF.

[3] Directive 95/46/EC of the European Parliament and of 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, OJ L 281 of 23/11/1995, pages 31 - 50, found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

for the proper functioning of a website are exempt.[4] The Article 29 Working Party (i.e. the privacy advisory body for the European Commission, having representatives of the regulators from the 27 EU member states) published an opinion on cookie consent exemptions. It identified seven types of cookies that are not subject to the requirement, including session ID cookies, load balancing session cookies and authentication cookies.[5]

The Article 29 Working Party has identified seven types of cookies that are not subject to the consent requirement.

If the data collected by a cookie is personal data (i.e. information traceable to an individual person), the other provisions in the 1995 Privacy Directive also apply in addition to the 2009 e-Privacy Directive.

Types of cookies

In determining the scope of Article 5:3 of the revised 2009 e-Privacy Directive, a distinction is usually made between three different categories of cookies: (i) technical cookies, (ii) analytics and statistical cookies, and (iii) tracking cookies.

Technical cookies are the cookies necessary to facilitate the use of a website. An example is a cookie that remembers the language stored by the user or that keeps track of which products a website user has put in his or her shopping basket before proceeding to payment. Security cookies are another example; these are used for online banking to support a secure connection with the customer. All of these cookies store information only during or for the user session.

---

[4] The exception is for "any type of technical storage for the sole purpose of carrying out the transmission of a communication over an electronic communication network or, if strictly necessary, in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

[5] Article 29 Working Party, Opinion 04/2012 on Cookie Consent Exemption, WP194, of 7 June 2012. Found at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

This list identifies the cookies for which consent is not needed for their placement and access:

1) User input cookies (session-id), for the duration of a session or persistent cookies limited to a few hours in some cases.
2) Authentication cookies, used for authenticated services, for the duration of a session.
3) User centric security cookies, used to detect authentication abuses, for a limited persistent duration.
4) Multimedia content player session cookies, such as flash player cookies, for the duration of a session.
5) Load balancing session cookies, for the duration of a session.
6) UI customisation persistent cookies, for the duration of a session (or slightly more).
7) Third party social plug-in content sharing cookies, for logged-in members of a social network.

Analytics and statistical cookies are cookies that, for example, count the number of unique visitors to a website or gather information about the surfing behaviour on a website. A discussion has arisen as to whether these cookies fall under the exemption of cookies necessary to facilitate the use of the website. Recently, the Dutch minister of justice has taken the position that the consent requirement does not apply for first-party analytics cookies that a website owner uses exclusively to collect data concerning the use of the owner's website in order to improve the functioning of that website.[6] The minister asked OPTA to identify further conditions for this, including in any case the condition that cookies may be used to collect only anonymised data not shared with third parties. The French privacy regulator, CNIL,[7] is of the opinion that cookies used exclusively during a user session to collect statistical information about the behaviour on the website are exempt from the consent requirement.[8]

Tracking cookies are cookies that collect data about the behaviour of users on the websites they visit. Such cookies are usually - either with the consent of, or at the request of, the website owner - placed by an advertising network. In this way, the advertising network collects large amounts of data, which is then used to draw up profiles of the users. These profiles are then "sold" to advertisers, in the sense that the advertisers, in exchange for payment, instruct the advertising network to show a certain advert to users with the purchased profile. The advertising network pays part of this income to the website owner who has given it consent or instructions to place the cookie. Advertising networks usually retain the profile data for a longer period (several years).

In general, it is assumed that consent must be provided before a cookie is placed or accessed.

Implementation in the Netherlands

The amended Article 5:3 of the 2009 e-Privacy Directive has been implemented in the Netherlands in the form of article 11:7a of the Telecommunications Act,[9] which entered into effect on 5 June 2012.[10] The concept of consent in article 11:7a of the Telecommunications Act

[6] Letter dated 20 December 2012 from Minister Kamp to the Dutch House of Representatives. Found at http://rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/12/20/kamerbrief-olver-analytische-cookies-en-artikel-11-7a-van-de-telecommunicatiewet.html.

[7] Commission nationale de l'informatique et des libertés. See http://www.cnil.fr/english/.

[8] CNIL, What the Telecoms Package changes for cookies. Found at http://www.cnil.fr/english/news-and-events/news/article/what-the-telecoms-package-changes-for-cookies/.

[9] Bulletin of Acts and Decrees 1998, 610.

[10] Act of 10 May 2012 to amend the Telecommunications Act for the implementation of the revised telecommunication guidelines, Bulletin of Acts and Decrees 2012, 235.

has the same meaning[11] as in article 1(i) of the Data Protection Act.[12] In this latter provision, consent is described as "any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal data relating to them". In general, it is assumed that consent must be provided before a cookie is placed or accessed.

Unambiguous consent?

Since then, various media and forums have reported that article 11:7a of the Telecommunications Act requires, in principle, unambiguous consent for tracking cookies.[13] However, this is not the case. The application of the Data Protection Act means that processing must be justified, but this does necessarily require consent.

Article 8 of the Data Protection Act also sets out seven factors that justify the processing of personal data, and one of these is unambiguous consent under paragraph (a). As emphasised in the explanatory memorandum accompanying this article, this justification is not exclusive, however, and data can also be processed in accordance with one of the other justifying factors stated in article 8.[14] Personal data may also be processed if any one of the other justifications stated in the article apply.

Asking data subjects for their consent has drawbacks. Consent can always be withdrawn. Consent is insufficient if there is an unbalanced relationship (e.g. employer-employee). In the Netherlands, article 8(f) of the Data Portection Act is usually the justification. This article states that personal data may be processed if this processing is necessary to promote the justified interest of the controller or a third party to which the data is provided, unless the privacy interest of the data subject prevails, to state it briefly. The controller must therefore balance these interests. This process must involve all relevant factors, including the level of sensitivity of the data, the amount of data and the measures used to take into account the interests of the data subject.

---

[11] Article 11:1(g) of the Telecommunications Act stipulates what is considered consent from a user or subscriber: "consent of a data subject as referred to in article 1(i) of the Data Protection Act, with the understanding that consent can also relate to data from subscribers who are not individuals."

[12] Bulletin of Acts and Decrees 2000, 302.

[13] According to the Dutch national government: "the law assumes that the party that places a cookie to track surfing behaviour does this to process personal data. This means that, as a rule unambiguous consent is required for cookies that track surfing behaviour". See http://www.rijksoverheid.nl/onderwerpen/ict/veilig-online-en-e-privacy/internetbezoek-volgen-met-cookies. The Cookierecht website states: 'tracking cookies fall under the privacy law and require explicit and unambiguous consent prior to their placement.' See https://cookierecht.nl/diensten/juridisch-advies/achtergrond-cookiewet/.

[14] Parliamentary documents II 1997-1998, 25892, no. 3, p. 80.

To the controller or advertising network, their interest in placing the cookie is justified under article 8(f) because it increases the income that can be generated with the collected data. This is not possible without tracking cookies. At the same time, the intrusion on the data subject's privacy is relatively minor. Moreover, data subjects can simply change their browser settings to remove cookies that have been placed.

In the parliamentary debate, the legal presumption was added at the last minute that the use of tracking cookies constitutes the processing of personal data.

Implicit consent

The importance of this interpretation is that it creates the possibility - even with the current wording of the first paragraph of article 11:7a of the Telecommunications Act - that implicit consent will be considered sufficient if the user is given clear and complete information about the cookies to be placed. Such an interpretation is also in line with the views of regulators in other countries.[15] The UK regulator, the ICO,[16] pointedly takes the position that implicit consent is sufficient, even for the placement of tracking cookies.[17] The ICO assumes that it is sufficient to place a banner or a bar on the website with a hyperlink linking the user to information about the cookies, along with a notice informing the user that, if the user continues to use the website, the user is consenting to cookie placement.[18]

At the present time, it is not a foregone conclusion that this type of implicit consent will also be considered sufficient in other countries such as the France and the Netherlands. The French privacy regulator, CNIL, emphasises in any case that the way of giving consent may differ

[15] Letter dated 20 December 2012 from the Justice Minister to the Tweede Kamer. Found at http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2012/12/20/kamerbrief-olver-analytische-cookies-en-artikel-11-7a-van-de-telecommunicatiewet/analytische-cookies-en-artikel-11-7a-van-de-telecommunicatiewet.pdf.

[16] Information Commissioner's Office. Found at http://www.ico.gov.uk/.

[17] ICO, "Guidance on the rules on use of cookies and similar technologies" (May 2012). Found at http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx.

[18] ICO, "Guidance on the rules on use of cookies and similar technologies", p. 20: "Some users might not [click on either "I agree" or "No thanks"] and go straight through to another part of the site. If they do, you might decide that you could set a cookie and infer consent from the fact that the user has seen a clear notice and actively indicated that they are comfortable with cookies by clicking through and using the site. This is an option that relies on the user being aware that the consequence of using the site is the setting of cookies. If you choose this option you might want the reassurance of a notice appearing elsewhere on the site which reminds users that you are setting cookies."

according to the intrusiveness of the cookie and therefore also recognises the possibility of implicit consent.[19] The Dutch regulator, OPTA, has posted a publication called "Frequently asked questions about the new cookie rules" that does not address the issue of whether implicit consent is sufficient under article 11:7a of the Telecommunications Act; however, nor is this possibility expressly excluded.[20]

The legal presumption does not mean that unambiguous consent is required for tracking cookies.

In its recent opinion about this issue, the Article 29 Working Party also does not exclude the possibility that implicit consent is sufficient:

> *The notion of "indication" is wide, but it seems to imply a need for action. … The requirement that the data subject must "signify" his consent seems to indicate that simple inaction is insufficient and that some sort of action is required to constitute consent, although different kinds of actions, to be assessed "in context", are possible.*[21]

In the ICO example described, clicking on a subsequent page after the information bar about cookies has been shown could be characterised as an "indication signifying consent".

The explanatory memorandum accompanying the amendment of article 11:7a of the Telecommunications Act recognises that consent can also be provided by a browser setting.[22] It was noted that the browsers available at that time (2010), which accepted all cookies as standard practice and had to be changed to refuse cookies, did not satisfy the consent requirement in Article 5:3 of the e-Privacy Directive. That article requires in any case an "expression of will" from the data subject that he or she wishes to accept the cookie in question. This can vary from cookie to cookie. The Article 29 Working Party was critical of this matter, and has furthermore indicated that the choice made by the user can be sidestepped (e.g. by flash cookies, which can

[19] The opinion of the CNIL is as follows: "The word 'agreement' thus clearly refers to consent as defined in article 2(h) of Directive 95/46/EC, that is to say to "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." See "What the Telecoms Package changes for cookies" (December 2011). Found at http://www.cnil.fr/english/news-and-events/news/article/what-the-telecoms-package-changes-for-cookies/.

[20] Frequently asked questions about the new cookie rules - update 2 August 2012. Found at http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3636.

[21] Article 29 Working Party, Opinion 15/2011 on the definition of consent, WP187, of 13 July 2012, p. 12. Found at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

[22] Parliamentary documents II, 2010-2011, 32549, no. 3, p. 80.

"reinstate" themselves after they are removed) and that the current browser settings give one-off consent for all future cookies, without the user being able to consider the purpose of these cookies on a case-by-case basis.[23]

For the rest, the business community has been working for several years on modifications to the most frequently used browsers. Compliance with the consent requirement in the Telecommunications Act is possible, but for the time being it should be assumed that the existing browsers are not suitable for this purpose.

Informed consent

Consent must be based on clear and complete information about the cookie. If the cookie is used to process personal data, the same requirement applies under articles 33 and 34 of the Data Protection Act. Regulators also emphasise the importance of providing sufficient information to data subjects in advance and of making this information easy to find.[24] There is some discussion about what information must be provided. If personal data are processed using the cookie, the provisions of article 33 and 34 of the DPA are applicable. These articles require that the identity of the controller and the purposes of the processing must be shared with the data subject, along with information needed to guarantee "proper and careful processing" for the data subject.

In consultation with the business community and OPTA, the Dutch division of the Interactive Advertising Bureau (IAB) has developed a three-step approach to the information to be provided to users.[25] The first step is a pop-up bar that appears as soon as a visitor comes to the website.

---

[23] Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, WP171, of 22 June 2010, p. 14. Found at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.

[24] ICO, *Guidance on the rules on use of cookies and similar technologies*: "The provider must ensure that clear and relevant information is readily available to users explaining what is likely to happen while the user is accessing the site and what choices the user has in terms of controlling what happens. (…) the text should be sufficiently full and intelligible to allow individuals to clearly understand the potential consequences of allowing the cookies should they wish to do so (…). Making sure users will see clear information about cookies is important for compliance with the information requirements of the Regulations, to ensure that consent is valid and more broadly to increase levels of user awareness." CNIL, *What the Telecoms Package changes for cookies*: "The validity of consent is linked to the quality of the provided information. It must be written in simple terms that are comprehensible to the general public, while being precise." OPTA, *Frequently asked questions about the new cookie rules - update* (2 August 2012): "Parties that place cookies and access them must provide clear information about the fact that they use cookies and for what purpose."

[25] 1AB, Industry-wide informational texts. Practical guidelines so that your organisation too can comply with the statutory information obligation in accordance with the Cookie rules in the Telecommunications Act (art. 11:7a). Found at http://www.iab.nl/wp-content/uploads/downloads/2012/11/Guide-Industriebrede-

This bar states that the website uses cookies and offers a link to additional information. Visitors who click on this link are given a short explanation about the cookies used on the website. This explanation is general in nature and does not distinguish between the different types of cookies. After this, users can click through to a page with a detailed explanation about the cookies used on the website. This sets out the cookie categories based on the information collected and the purposes for which the information is used. This is followed by a list of all the cookies used on the website, along with the party that has placed each cookie, the associated information category of that cookie, and the length of time that the information is retained. It is plausible that this satisfies the information requirement, although from this information it is not possible to identify which categories of people the information is provided for.

Browsers that accept all cookies as standard practice do not satisfy the consent requirement.

Cookies in the 2012 proposal for amendments to the privacy regulation

The cookie regime in the e-Privacy Directive will become even stricter if the proposal published on 25 January 2012 for the new privacy regulation[26] becomes law. Article 20 of the proposed regulation states that profiling requires the consent of the data subject. On this basis, consent is no longer linked to the processing of personal data, but is required for all automated processing of data intended to evaluate certain aspects of the personality of an individual or, in particular, to analyse or predict this person's professional performance, economic situation, place of residence, health, personal preferences and reliability of behaviour. This means that, in principle, consent will be mandatory for all tracking cookies and analytics cookies. Consent is defined as follows: "any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal data relating to them, whether by means of a statement or an unambiguous active act". With respect to the current definition in article 1(i) of the Data Protection Act (see the previous sentence), it is notable that there must be an explicit expression

Cookie-informatieteksten.pdf.

[26] 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), 25/1/2012, COM(2012) 11 final.
Found at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

of will, by means of a statement or an unambiguous active act. If this text is adopted, implicit consent will probably no longer be sufficient.

If this text is adopted, implicit consent will probably no longer be permitted.

Tips & Tricks (in general terms)

1. Determine which cookies are used.
2. Distinguish between technical, analytics and tracking cookies.
3. Place a bar, banner, pop-up, etc., on the website with:
   a. a brief notice that cookies are being used;
   b. a button or area where consent can be given; and
   c. a hyperlink to additional information about cookies.
4. Under the hyperlink: information about the cookies used and the possibility of accepting each cookie.
5. If no consent is given, refrain from cookie placement.
6. State on the bar, etc. (see point 3) that, if the user continues to use the website, this constitutes consent to use all cookies.[27]

[27] OPTA must still issue a statement concerning whether implicit consent, as proposed here, is permitted.

PRIVACY IN THE CLOUD

5

Cloud computing entails the saving, processing and using of company data on the servers of a cloud provider instead of on servers located at the company's premises. Cloud providers may also offer software and hardware the company can access online after logging in. The company pays for this service in a number of different ways: per storage unit, per user, or per unit of time (or a combination of these).

In 2006, both Amazon and Google began, almost simultaneously, to use the term "cloud computing". These two companies had servers throughout the world, but server capacity was not being fully utilised during much of the day. To increase the returns on these servers, these companies started offering capacity to third parties as a place to store their data and software. To achieve maximum returns, the data was always placed on the server that had space available at that time. This location shift has become the determining factor for the concept of cloud computing.

For many companies, it is important to control their data at all times. Financial institutions and other companies under the supervision of the Dutch central bank, De Nederlandsche Bank (DNB), must always exercise control over their data and ensure that the cloud provider complies with the regulatory legislation. This is required by the Financial Supervision Act and the Decree relating to Prudential and Valuation Rules in the Financial Supervision Act.[1] The continual shifting of the data 's actual location, as determined by the cloud provider, makes this control more difficult. DNB must be able to have access to this data at any point in time. This factor is not compatible with a constant shift in data location. Moreover, the cooperation of the cloud provider is required for this obligation to be met. Finally, the location of the data - and especially the location shift - is an important aspect in complying with the statutory privacy rules.

To meet these needs, models of cloud computing arose in which the company could more or less determine the locations where the data was held. If the servers are intended for a single company, this constitutes a private cloud. There is little or no difference between this and a situation in which the hosting of data processing is outsourced. DNB has indicated that it considers cloud computing a form of outsourcing.[2] DNB must be informed in advance of a company's intention to use cloud

DNB has indicated that it considers cloud computing a form of outsourcing.

[1] Decree relating to Prudential and Valuation Rules that implements article 3:18 of the Financial Supervision Act, arts. 27 to 32a.

[2] Circulaire cloud computing [Cloud computing circular], De Nederlandsche Bank, dated 6 December 2011. Retrieved 27 March 2013 from http://www.toezicht.dnb.nl/binaries/Cloud%20computing_tcm50-224828.pdf.

computing, and the company concerned is required to submit a risk analysis to DNB.[3]

Advantages and disadvantages

Cloud computing offers companies a number of advantages. The cloud provides flexibility, i.e. if server space or other software or hardware is needed, the company does not have to purchase these, but in principle can rent them on demand. This allows companies to save money on purchasing and energy expenses, as well as on office space and, in some cases, on IT staff. Servers are now operational expenses instead of capital costs.

In a recent study, the European Commission calculated that by 2020 the European market for cloud computing will be able to generate a total of EUR 160 billion annually in savings and productivity improvements. The study on which this is based revealed that companies can save an average of 10% to 20% on their IT costs through cloud computing.[4] Cloud computing is therefore more of a financial than technological phenomenon. The main disadvantage of cloud computing is that the company must depend on the cloud provider to a large extent for the company's operations. This becomes even more significant if a majority of the IT staff disappears. This dependence gives rise to questions about the associated risks and how control and management can be retained as far as possible.

Several questions must be addressed by a company's in-house legal counsel:

- How can it be guaranteed that data and software will always be accessible and available?
- How can sufficient security be enforced and controlled?
- On termination of a cloud contract, how can a seamless transition to a new provider be ensured so that no data are left behind?

The answer to these questions is relatively simple, but can also be difficult in practice. The simple answer is to find a provider that offers the necessary guarantees with respect to access, availability, control and security. Create an exit plan that states what must happen upon termination of the relationship and how the data will be transferred. And make sure to record this properly in a contract.

What is difficult is that many cloud providers work with standard contracts that cannot be negotiated (or only to a minor extent). The most economical cloud services do not provide any

[3] See J.M.A. Berkvens, "Clou(d)(t)sourcing binnen de financiele sector" [Cloudsourcing in the financial sector], Tijdschrift voor Financieel Recht 2012/12, p. 444 et seq.

[4] Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake, D4 – Final Report, IDC, 13 July 2012. Found at http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf.

guarantees at all, and liability is virtually fully excluded. More expensive cloud computing models offer the company more security about the quality of the services provided and the accountability of the provider often entails negotiable guarantees and access rights. In addition, it is frequently possible to arrange for the data to remain in the EU, or even in the Netherlands. Such a cloud provider may even be willing to accept the usual liability, enforced by a penalty clause.

Privacy

Going "into the cloud" also raises the question of how a company can comply with applicable privacy legislation if the data are located in another country.

In 2012, this issue received attention in European privacy legislation. A recent publication of the European Commission, "Unleashing the potential of cloud computing in Europe", reports that research has revealed that the greatest barrier facing companies considering cloud computing is privacy.[5] The Article 29 Working Party (the European Commission's privacy advisory body, having representatives from the regulatory bodies of the 27 EU member states) stated in its opinion on cloud computing and privacy that a lack of control over the data and insufficient information about the processing of the data are major obstacles.[6] The European Data Protection Supervisor (the privacy regulator for European institutions and also the independent data protection adviser to the Commission and the European Parliament) has set out its views on the privacy aspects of cloud computing in a recent opinion in response to these two documents.[7]

According to the European Commission, privacy concerns form the largest barrier for companies that are considering cloud computing.

The most important development for cloud providers and their customers is undoubtedly the proposal, published on 25 January 2012, for new privacy regulation[8] expected to replace the

[5] "Unleashing the potential of cloud computing in Europe – What is it and what does it mean for me?" European Commission, 27 September 2012. Found at http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.

[6] Article 29 Working Party, Opinion 05/2012 on Cloud Computing, WP 196, 1 July 2012. Found at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[7] Found at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.

[8] 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.

1995 Privacy Directive.[9] The expectation is that it will be several years before this regulation enters into effect, but the storm clouds are already gathering.

The ability of the CBP to impose sanctions will be greatly expanded if the proposed regulation is adopted in its current form.

The most striking change will be the strongly expanded powers of member state regulators found in Article 53 of the proposed regulation. In the Netherlands, the regulator is the Dutch Data Protection Authority (Authority). Under current privacy legislation, the Authority has limited powers to conduct investigations and impose sanctions. These powers will be greatly expanded if the proposal for the new regulation is adopted in its current form.

In this event, the Authority will not only be able to prohibit the processing of certain data, but also be given far-reaching investigative powers similar to those enjoyed by competition watchdogs, such as the Netherlands Competition Authority (NMa). These powers could be exercised in "dawn raids" similar to those currently conducted for suspected competition violations. This would involve the regulator paying an unannounced visit to corporate offices, searching for evidence of criminal acts, demanding access to the IT infrastructure, and making copies of all the relevant data.

Fines

To strengthen the enforcement of the privacy rules, the Authority and its European counterparts will be given the option of imposing heavy fines for regulatory violations. The maximum fine will amount to 2% of a company's annual worldwide turnover, under Article 79:6 of the proposed regulation).

Particularly important to the context of cloud computing, under Articles 40 to 44 of the proposed regulation, it will become possible to impose a fine for the illegal transfer of data to a country outside the EEA. A transfer of this kind can easily occur in the cloud if the relevant agreements and measures are inadequate. In principle, it is the cloud provider that decides where the data is stored.

These penalty provisions emphasise that a company considering moving its data into the cloud must make certain (e.g. by obtaining contractual guarantees) that the cloud provider will comply

[9] Directive 95/46/EC of the European Parliament and of 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, OJ L 281 of 23/11/1995, p. 0031 – 0050.

with the privacy rules and that the company will be able to supervise compliance by means of unannounced audits.

What makes this particularly important is that, under Article 26 of the proposed regulation, the company (as the controller) will be liable for any violation of the privacy rules, even if the fault lies with the cloud provider.

Contractual agreements

The French privacy regulator, CNIL,[10] recently published a number of recommendations[11] for companies that plan to use cloud computing.

A risk analysis should be performed in advance. It should be established whether the data to be stored in the cloud by the company is sensitive in nature, because if so additional requirements apply.

The following should also be determined:

- what are the legal and technical conditions that the processing must comply with?
- what are the main risks?
- what measures are needed to limit these as much as possible?

As for outsourcing, it should be determined whether the company retains sufficient in-house IT knowledge to ensure that it is not completely dependent on the cloud provider, and also how the data (and possibly the IT staff) are returned to the customer at the end of the contract.

The analysis should also address the measures taken by the cloud provider to guarantee the confidentiality of competition-sensitive information, such as unpublished turnover and profit figures and information about acquisitions and competition issues.

Finally, an assessment should be made of whether the cloud provider makes it possible for the company to comply with specific sector-related conditions, such as the security and supervisory requirements imposed on financial institutions by DNB. Involving lawyers in the performance of these analyses and the recording of guarantees in the contract is vital.

---

[10] Commission nationale de l'informatique et des libertés. See http://www.cnil.fr/english/.

[11] Recommendations for companies planning to use Cloud computing services, 25 June 2012. Found at http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf.

Foreign legislation

Another legal risk that must be considered is that in the US and some other countries the government has the legal power to demand access to the data on the provider's server, and the provider must grant that access.

The US Patriot Act[12] is often cited in this context. This act expanded the existing powers of the FBI and other intelligence agencies to gather data about citizens, including from cloud providers, in order to combat terrorism and foreign espionage. Similar powers are also available under the US Foreign Intelligence Surveillance Act (FISA), amended in 2008, which was extended by President Obama in late 2012 for an additional five years. Under FISA, cloud providers can, for example, be required without a court order to provide information about certain people residing outside the United States.[13]

Involving lawyers in the analysis of cloud computing risks and the recording of guarantees in the contract is vital.

Both acts focus primarily on combating international terrorism, sabotage and counterintelligence; however, they offer virtually no safeguards for the company or person to whom the information relates. While it appears that the powers provided for in the Patriot Act and the FISA have been used only to a limited extent, there is significant resistance in Europe to the use of cloud providers in the US mainly because of the possibility of information being shared with the intelligence agencies without the data subjects' knowledge.

To put this issue into perspective, however, it is pointed out that in every European country the government has similar powers. In 2011, Dutch government investigators requested traffic data from telecom providers 2.3 million times.[14] This does not include information requests made by the Dutch General Intelligence and Security Service and the Dutch Military Intelligence and Security Service.

---

[12] Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001. Found at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf and http://www.justice.gov/archive/ll/highlights.htm.

[13] 50 USC § 1801 et seq; Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISAAA), HR 6304.

[14] CIOT inquiries. Process and legality; Ministry from Security and Justice, November 2012. Found at http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/12/20/ciot-bevragingen-proces-en-rechtmatigheid.html.

However, the US legislation does extend further than Europeans are used to in the following ways:

- Data can be obtained not just from cloud providers located in the US, but also from their foreign group companies and even from cloud providers that structurally do business in the US but have no branch there.
- There is no advance court review process. Nor is the consent of the public prosecutor required.
- The cloud provider may not inform the customer concerned of the request.
- Information may be shared with other government agencies.

The data that can be obtained from a cloud provider are, in principle, limited to subscriber data, invoices and traffic data, including the e-mail addresses used. The contents of the e-mails may not be requested. However, in practice, the US intelligence agencies do not always abide by these restrictions. Moreover, the fact of the matter is that a company has no control whatsoever on the use of these powers under the Patriot Act.

Furthermore, no exemption is made in the proposed regulation for a transfer made in accordance with an order by a US intelligence agency. Consideration 90 simply states that transfers "should only be allowed where the conditions for transfer to third countries are met". Even though a controller is not even aware of the transfer, a transfer made under the Patriot Act does not fall under the exceptions set out in Article 42 (model clauses), Article 43 (binding corporate rules) or Article 44 of the proposed regulation. These provisions all assume the controller is aware of, and involved in, the transfer.

An unauthorised transfer by the cloud provider could result in the company receiving a fine of a maximum of 2% of annual group turnover.

If the proposal becomes law, and if the letter of the new law is followed, an unauthorised transfer by the cloud provider in these circumstances could result in the company being fined a maximum of 2% of the annual group turnover. In practice, however, this is unlikely to happen, because after all it is not the controller that would be violating the regulation by transferring personal data or by giving instructions to this end.

Since it is known that there is a risk of US intelligence agencies requesting corporate information from a cloud provider, without the company's knowledge, the question that arises is whether a company having that knowledge can fully exculpate itself in that situation. After all, Article 26 of the proposed regulation stipulates that a controller that has a third party (including a cloud

provider) process personal data must, when selecting a processor, enter into an agreement that guarantees that the processor will comply with European privacy law (to state it briefly). A cloud provider subject to the Patriot Act - and there are many of them - will be unable to provide such a guarantee. If a US intelligence agency requests data, the cloud provider will have to provide this data - or risk criminal prosecution and heavy fines. Given these options one may assume that the cloud provider will cooperate with the request. In view of the above, for a company looking for a cloud provider, the Patriot Act may be a powerful disincentive to hire a cloud provider located in the United States. Further, a cloud provider with a subsidiary in the US, or a cloud provider that makes use of a cloud provider located in the US, is or may also be subject to the Patriot Act. Accordingly, the possibility of US intelligence agencies requesting data continues to be an important issue for Dutch companies selecting a cloud provider.

Tips & Tricks for selecting a cloud provider

- What data and/or software will go into the cloud?
- What are the main risks?
- What measures are needed to limit these risks as much as possible?
- Are there legal or contractual limitations on the use of the cloud?
- Where is the cloud provider located, and do the intelligence agencies in that location have the authority to request data from the cloud provider?
- With which legal and technical conditions must the cloud provider's processing operations comply?
- Will sufficient IT knowledge remain in house to ensure the company is not completely dependent on the cloud provider?
- Are there sufficient guarantees for availability and 24/7 access?
- Has the cloud provider taken sufficient security measures to combat unauthorised access and data breaches?
- Can an audit be conducted at any point in time to check whether the cloud provider is complying with the agreements?
- Are the regulator's legal audit rights guaranteed?
- Have proper arrangements been recorded on behalf of the company for the processing of the personal data (what data are processed, where and with what purpose, for how long and who has access to the data)?
- Has consent been obtained from employees and the works council for the processing of employee medical data and other sensitive data (whistleblower procedures)?
- Is the cloud provider required:
  - to comply with requests from data subjects to provide information on their data, or for the rectification or protection of their data?
  - to report data breaches and cooperate with the investigation and the measures to be taken?
  - to cooperate with data protection impact assessments of processing operations that are accompanied by special risks to privacy?
- Is there a good exit scheme to ensure a seamless transition to a new provider?

E-DISCOVERY AND PRIVACY: THE ETERNAL DILEMMA?

E-Discovery is the provision of electronically stored data to the other party and to the court in civil proceedings and to the regulator in the context of an investigation.

Increasingly, Dutch companies are involved in American litigation and government investigations. They often involve a common-law litigation process called "discovery", i.e. the disclosure by a party of relevant facts or documents. For information stored electronically (which is now most information), the process is often referred to as "e-Discovery".

Litigation or an investigation may result in a Dutch company becoming directly involved in the discovery process; however, a company may also become indirectly involved if the litigation or investigation concerns a group company.

A Dutch company may also be able to take advantage of the American discovery process in Dutch proceedings (whether as the plaintiff or defendant). In certain circumstances, a Dutch company may be able to make use of the discovery procedure in the United States in order to obtain certain documents from the other party. This is not prohibited by Dutch civil procedure and, in principle, would not conflict with the choice of jurisdiction or other civil procedural rules and requirements.[1]

Ultimately, the court establishes in a discovery order the scope and the limitations of the information to be submitted.

In the context of civil litigation, Rule 26 of the US Federal Rules of Civil Procedure (FRCP)[2] stipulates that a company must, for the purposes of discovery, make available to the other party and the court all documents, electronically stored information and materials in its possession or under its control and which concern its claim or defence. This includes e-mails, recommendations and memorandums, but also, for example, the telephone communication data for the people involved. There is a limit to the data that can be collected in this manner: information not reasonably accessible because of the disproportionate effort or costs involved need not be

[1] Rotterdam Court, 8 August 2012, JBPR 2012 vol. 5, with note by R.B. van Hees and P.J. van der Korst.

[2] Federal Rules of Civil Procedure, with forms, 1 December 2010. Publication of the Judiciary Committee, House of Representatives. Found at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2010%20Rules/Civil%20Procedure.pdf and http://www.law.cornell.edu/rules/frcp/.

disclosed. In principle, privileged information (legal advice and correspondence with the lawyer) and company secrets are excluded from the discovery process. The parties are required to jointly present a discovery plan to the court, which sets out the information to be submitted and the form in which this must be made available. The submitting party will naturally attempt to limit the amount of information to be submitted; wheras the other party will want to receive as much information as possible. An American court issues a discovery order setting out the scope and the limitations of the information to be submitted.

If one of the parties does not disclose certain information, the court may draw appropriate conclusions. In practice, this generally means the court will assume the undisclosed information contains proof of the other party's arguments and may allow those arguments. Furthermore, in this event, a court can award "treble damages", especially if it seems that the information was intentionally destroyed or not disclosed. Under Rule 37 of the FRCP, the court will not impose sanctions if the information is not available as a result of the routine and bona fide functioning of an electronic information system. Partly because of this reason, it can be extremely important for a company to have a good and consistently implemented document retention policy. (See also the chapter entitled "Document retention: data storage and retention periods".)

A company has comparable disclosure obligations if it comes under investigation by a US regulator, including pursuant to the Foreign Corrupt Practices Act (FCPA),[3] the Code of Federal Regulations,[4] the Foreign Asset Control Regulations,[5] the Sherman Antitrust Act[6] and the Sarbanes-Oxley Act (SOX).[7]

In many cases (e.g. whistleblower procedure or audit), the company will be the first to know of a violation. In this event, the company is required to report this to the competent regulator and make the relevant information available.

---

[3] United States Code (USC), Title 15 § 78dd1. Found at http://www.law.cornell.edu/uscode/text/15.

[4] Several laws forbid the export of military goods and goods that can be used for military purposes.

[5] Code of Federal Regulations, Title 31 - Money and Finance: Treasury; Subtitle B - Regulations relating to money and finance; Chapter V - Office of Foreign Asset Control, Department of the Treasury. Contains export restrictions and sanctions for trade and financial transactions with certain countries. Found at http://www.treasury.gov/resource-center/sanctions/Pages/CFR-links.aspx.

[6] 15 USC §1-7, under the heading "15 USC Chapter 1 - MONOPOLIES AND COMBINATIONS IN RESTRAINT OF TRADE". Retrieved 28 March 2013 from http://www.law.cornell.edu/uscode/text/15.

[7] Sarbanes-Oxley Act (SOX) contains, among other things, rules for controlling the dissemination of price-sensitive information and rules for internal control and financial reporting. It applies to listed companies in the United States (as well as their group companies abroad).

Disclosure as a violation of privacy

If a document to be disclosed contains personal data, disclosure may result in the company violating its obligations under the Dutch Data Protection Act (Act).[8] According to the legal definition of "personal data", personal date is any data traceable to an individual. This includes name, address, e-mail address, telephone number and vehicle plate number. According to the Article 29 Working Party (i.e. the privacy advisory body of the European Commission, having representatives of the regulators from the 27 EU member states), personal data also encompasses such things as the IP address automatically assigned to a computer connected to the internet and traffic data for mobile phones.[9] Furthermore, if an individual is identifiable from the context of the information, or by the combination of information, this too may constitute personal data.[10] The Act applies to each processing operation involving personal data, including not just the collection of such data, but also its storage, processing and further dissemination.

If the documents to be submitted contain personal data, a company may be in conflict with its obligations under the DPA.

Whether the data actually relate to private matters or not is irrelevant. Business e-mail addresses are considered personal data, which means that, in principle, all business e-mails contain personal data. That also applies to advisory documents (because of the names of the people to whom they are directed) and meeting reports (because of the names of the people present). Log files with data relating to the use of a certain computer also contain personal data, because the administration number of that computer can be traced to a work location and therefore also to an individual user.

Virtually all documents to be disclosed in the context of the modern-day discovery process contain personal data that is protected as private under the Act. The Act has a number of provisions that can complicate or delay compliance with the discovery process, as a result of which a Dutch company may not be able to comply, or fully comply, with a discovery request within the appropriate timeframe. The consequences of this are very serious in American litigation, whereas the sanctions imposed by the Act are relatively minor in comparison. Because

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

[9] Article 29 Working Party, opinion 4/2007 on the concept of personal data. (WP 136), established on 20 June 2007. Found at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[10] For these "indirectly identifying data", see the explanatory memorandum accompanying the bill for the Dutch Data Protection Act, Tweede Kamer 1997-1998, 25892, no. 3, p.48.

of this, there is a tendency to ignore the Act with this conflict arises.[11] However, there is no reason for this, because with proper preparation e-Discovery can be arranged in such a way that the company can both make disclosure and comply with the Act. In the near future, once the proposal published on 25 January 2012 for a new privacy regulation[12] takes effect ("proposed regulation"), the fines for violating European privacy rules will increase drastically. Under Article 79 of the proposed regulation, a violation of a provision (discussed further below) may be punishable by a maximum fine amounting to 2% of the annual worldwide turnover of the company.

Legal basis

Under Dutch law, the processing of personal data requires a legal basis. Article 8 of the Act identifies the consent of the data subject as the first legal basis; however, obtaining consent will be impractical and often impossible, especially in the context of e-Discovery involving a number of people.

The consent of an employee is insufficient. The Article 29 Working Party indicated in a 2009 opinion on pre-trial discovery that it is not an option for an employer to ask for an employee's consent in view of the subordinate position of an employee. Such consent is not considered to be freely given.[13] Article 7(4) of the proposed regulation expressly excludes this possibility, because there is a "significant imbalance" in the relationship between employer and employee. As a result, an employee's consent cannot form a justification for processing his or her personal data.

With proper preparations, e-Discovery can be arranged in such a way that the company can also comply with the provisions of the DPA.

Furthermore, the justification that the processing of personal data is necessary for the controller

[11] The Dutch Data Protection Act, art. 75(1), states that failure to comply with the obligation to report the processing of personal data may result in a third-category fine (€8,700). Under art. 75(2), if the violation is intentional, the maximum fine is €19,500.

[12] 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), 25/1/2012, COM(2012) 11 final.
Found at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[13] Article 29 Working Party, Working Document 1/2009 on Pre-trial discovery for crossborder civil litigation, WP158, of 11 February 2009, p. 8.
Found at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf.

(i.e. the company involved) to fulfil its obligations cannot be relied on, according to the Article 29 Working Party. The reason is that this justification exclusively applies to the legislation and legal measures of member states.[14] A discovery request made in the context of civil litigation does not fall into this category, so the justification is inapplicable. The Article 29 Working Party believes that complying with a discovery request, however, can be based on the justification set out in article 8(f) of the Act (i.e. "upholding...legitimate interests") because compliance is necessary to uphold the controller's legitimate interests. In any case, according to the Working Party, in each individual case (i.e. for each individual document), a determination must be made whether that interest overrides the data subject's fundamental right to privacy protection.[15]

The proposed regulation states that the Commission can establish additional rules for sectors and situations with respect to data processing to further establish the practical aspects of this basis.[16] In response to this (the Albrecht Report published in January 2013), the rapporteur of the European Parliament proposed significantly limiting this basis.[17] After considering the interests involved, if a controller decides that its legitimate interests outweigh the privacy interests of the data subject, the controller must inform the data subject of this, and provide the associated reasons. The Albrecht Report states that a company's legitimate interest is not the overriding factor if the processing leads to a serious risk of harm to the data subject or if a large number of people will have access to the data subject's personal data.[18]

Proportionality principle

Proportionality is an important principle in the Dutch Data Protection Act. The main idea is that personal data may be processed no more than necessary for a specific goal. That requires an intentional filtering of the documents, and the associated personal data contained in these documents, that are submitted for e-Discovery purposes. Personal e-mails and documents will have to be deleted and, where necessary and possible, personal data will have to be redacted in the documents to be submitted.

Personal data may be collected only for a specific and clearly described purpose (Act, art. 7). In principle, personal data cannot be processed for a purpose incompatible with this (Act, art. 9).

---

[14] Article 29 Working Party, WP158, p 9.

[15] Article 29 Working Party, WP158, p 9.

[16] Proposed regulation, Article 6(1)(f)

[17] Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual 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.

[18] Albrecht Report, p. 71-73 (Amendments 100-102).

At first glance, this can give rise to complications in connection with a discovery request. For example, employees' personal data are in any case processed in the framework of their activities for the company. The purpose of this process is not to make these data available to third parties for discovery purposes. However, it can be argued that these purposes are compatible, because providing an e-mail inbox or electronic file (with the abovementioned personal data) to comply with a discovery request, and also submitting the original e-mails and documents, serves the objective of the company.

It is essential that the documents be selected by independent experts who possess the required knowledge and experience.

In practice

The practical aspects of the e-Discovery process must be guided by in-house legal counsel or the compliance officer, and preferably be performed by a team that includes the company's US counsel and its Dutch counsel. In connection with employee-related aspects, including an HR manager in the team can also be useful.

It is essential that the documents be selected by independent experts who possess the required knowledge and experience, so that errors (which can have serious consequences in American litigation) are prevented. Some companies, called "e-Discovery providers", now specialise in assisting with the e-Discovery process. An e-Discovery provider, which has special software for searching electronic files very quickly and expertly for relevant information, can be very valuable in this process. The actual investigation of data files and, in particular, locating the relevant e-mails and documents will therefore be done by this e-Discovery provider. Using an extensive thesaurus of key words, this provider will be able to distinguish between documents that contain privacy-sensitive information (such as an employee's personal e-mails) and purely business documents. This is needed to ensure that the processing of personal data - and particularly the transfer of data to the United States - complies with Dutch law.

For personal e-mails and other documents that contain privacy-sensitive information, it may be necessary to look at each individual document to see whether it is a personal document or whether it (also) contains information relevant to the case. In addition, the proportionality principle can be complied with by filtering the data to be provided for the discovery request in advance for relevance, after removing the non-relevant personal e-mails and personal documents. It must then be determined which personal data are necessary and which information can be submitted in edited form (for example, with the personal data blacked out). In connection with the proportionality principle, this filtering and editing should preferably be performed in the Netherlands before the transfer of the data to the United States, where

additional requirements will be imposed (as described further below).

Transfer of personal data to the United States

The Act imposes strict rules on the transfer of personal data to countries that do not have the same level of personal data protection as the EU.[19] The European Commission has identified countries considered to have an adequate level of protection.[20] The United States is not on that list. In principle, transfer to the US is permitted if the recipient has agreed to comply with a programme called "Safe Harbor".[21] In so doing, this company accepts the obligation to put into practice the seven Safe Harbor Privacy Principles, including the obligation to inform data subjects if information about them is being collected and processed, the right of data subjects to refuse to have information shared with third parties, and the obligation, if data are transferred to third parties, to submit these principles to the third recipient. If it emerges that a company has not followed these principles, the Federal Trade Commission may impose a maximum fine of $12,000 per day.

In the context of a discovery or investigation, however, the Safe Harbor programme will often be inadequate. Under the Federal Rules of Civil Procedure[22] (or, for an investigation, the FCPA[23] or other relevant legislation), the company involved is in any case required to make available all the relevant data to the other party, the court and the investigative agency. These are usually not "Safe Harbor certified".

In the context of a discovery or investigation procedure, the Safe Harbor regime will often not be adequate for the transfer of personal data to the US.

Given the large amount of data that can be involved in e-Discovery, a test was developed in the case of Zubulake v. UBS Warburg to determine the scope of the documentation to be

[19] Dutch Data Protection Act, art 77.

[20] Andorra, Argentina, Australia, Canada, Switzerland, Israel, Faroe Islands, Guernsey and Isle of Man (on 1 Feb 2013).

[21] US-European Safe Harbor framework. Found at http://export.gov/safeharbor.

[22] See footnote 1.

[23] See footnote 2.

submitted.[24] When appearing in American courts, European companies have regularly invoked national "blocking legislation", including privacy legislation, in attempts to limit or prevent the disclosure of documents. American courts, however, have demonstrated little respect for such statutes, whether they relate to bank secrecy, business secrets or privacy. Such blocking statutes are seen by American courts as having the primary goal of prohibiting or limiting the submission of documents to a foreign court or a regulatory institution, even if there is an order to do so. These statutes are perceived as making it possible for European companies to evade the strict obligation to produce exhibits in the discovery process that is an integral part of American litigation.

In Société Nationale Industrielle Aerospatiale,[25] the American court applied a test in which more weight was given to compliance with the blocking statute. According to this test, if an American court believes that a European company is not running a serious risk of legal action being taken against it because disclosure violates the blocking statute, the European company's reliance on the blocking statute is rejected.[26] The importance of establishing the truth (which is the main point of disclosure in American litigation) and the interests of the other party are therefore usually overriding factors.

Both the US and the Netherlands are party to the Hague Evidence Convention.[27] The argument that the procedures set out in the Hague Evidence Convention must be followed is usually not accepted by an American court.[28] Under the Hague Evidence Convention, the gathering of

---

[24] Zubulake v. UBS Warburg, 216 F.R.D. 280 (S.D.N.Y. 2003). This test consists of the following factors:
1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.

[25] Société Nationale Industrielle Aerospatiale v. U.S., District Court for the Southern District of Iowa, 482 U.S. 522 (1987).

[26] Bodner v. Paribas, 202 F.R.D. 370, 375 (E.D.N.Y. 2000); Strauss v. Crédit Lyonnais S.A., 242 F.R.D. 199 (E.D.N.V. 25 May 2007); Gucci America, Inc. v. Curveal Fashion, 2010 WL 808639 (S.D.N.Y. 8 March 2010; Air Cargo Shipping Services Antitrust Litigation, 2010 WL 2976220 (E.D.N.Y. 23 July 2010).

[27] Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, The Hague, 18 March 1970 (Treaty Series 1979, 38).

[28] Société Nationale Industrielle Aerospatiale v. U.S., District Court for the Southern District of Iowa, 482 U.S. 522 (1987).

evidence by Dutch courts at the request of a foreign court for the benefit of proceedings before that court would be subject to the Dutch law of evidence. However, the Netherlands, Germany, France and Spain have made a reservation for - stated briefly - compliance with discovery requests. The alternative available under the Hague Evidence Convention therefore cannot be relied on during the discovery process in American litigation under the FRCP.

However, the US courts have demonstrated that they are willing to take European privacy legislation into account if highly privacy-sensitive documents are involved.[29] It is important for Dutch companies disclosing documentation in the scope of discovery or an investigation to do so in accordance with privacy legislation as much as possible.

The US courts have demonstrated that they are only willing to take account of European privacy legislation for documents that are highly privacy sensitive.

The transfer of personal data to the United States is also justifiable on one of the grounds referred to in article 77(1) of the Act. Under article 77(1)(d), transfer is justifiable if necessary for the establishment, exercise or defence in law of any right. In this case, the Dutch company must also enter into a standard contract with the recipient in the United States (usually its American lawyer), as required by the European Commission.[30] However, this does not contain a requirement for the American lawyer also to enter into a standard contract with the other parties who receive the documents from the lawyer (i.e. the court, the other party and experts).

[29] See, for example, In re Vitamins Antitrust Litigation, 2001 US Dist. Lexis 8904.

[30] Standard contract between two controllers: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (2001/497/EC). Found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:EN:HTML, as amended by the Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/EC/915). Found at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF. Standard contract between the controller and the processor: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12 February 2010, p. 5.

Other obligations under the Dutch Data Protection Act

Under article 33 of the Act, people about whom data is collected must be informed in advance of the associated purpose (and other matters).[31] Article 43 of the Act contains a number of grounds on which a controller may refrain from informing a data subject (which in the context of e-Discovery, applies in particular to employees and business relations). For example, the ground in art. 43(e) of the Act is that non-disclosure is necessary to protect the rights and freedoms of others, including the controller. In order for the e-Discovery to be made within the set timeframe, informing the data subjects after the fact is justifiable. In the event of an investigation by a regulatory institution, informing a third party will usually not be permitted . In that case, art. 43(d) may provide a basis for a delay in informing the data subjects, because this is necessary in connection with overseeing compliance with certain legal rules.

It is justifiable to only inform the data subjects afterwards in order to perform the e-Discovery within the set timeframe.

Another obligation set out in article 27 of the Act is that every processing of personal data must be reported to the Dutch Data Protection Authority (Authority). This is an administrative requirement that the Authority monitors and enforces only on a random basis. Exceptions to the notification requirement are set out in the Dutch Data Protection Act Exemption Decree (DPAED).[32] The processing of personal data in the context of discovery or an investigation may fall under the exception set out in article 15(3)(e) of the DPAED for lawyers who may process data "with a view to handling the case or settling the dispute". If not, the processing must be reported.

Proposed regulation

Under article 42 of the proposed regulation, transfer to third countries within a group of companies will be possible in the future under "Binding Corporate Rules". This cannot be used in a discovery procedure or an investigation.

Data may however be transferred to the United States on the basis of standard contractual provisions, such as those already established by the Commission in the framework of the

[31] In practice, it does indeed occur that the employment contract or the labour regulations applicable to all employees may include a provision that states that the personal data of employees also can be processed with a view to legal proceedings in or outside of the Netherlands. Based on the current rules, it is doubtful that this consent can be considered as "freely given" in view of the dependent position of the employee. In the light of the restriction of the concept of "consent" under the proposed regulation, consent will no longer be able to be used as a basis once this regulation takes effect.

[32] Bulletin of Acts and Decrees 2001, 250.

Privacy Directive. Furthermore, under article 44(1)(e), transfer may take place if necessary for the establishment, exercise or defence of legal claims.

However, the Albrecht Report proposes introducing a new article 43a into the proposed regulation that would place several limitations on the transfer of data for discovery procedures and investigations. According to that article, transfer would be possible only on the basis of a treaty between the European Union or a member state and the third country in question, such as the Hague Evidence Convention. If personal data are transferred, consent must be obtained in advance for the transfer from the regulator in the country from which the transfer takes place. (See article 43a(2) of the proposed regulation.) In addition, the controller or the processor in that case must inform the data subject of the request and the consent given by the regulator. Obviously, the amendments proposed in the Albrecht Report are still being discussed, as is the proposed regulation.

Under the proposed regulation, the penalty for a violation of the provisions governing transfer to third countries is much more severe than under the Privacy Directive. Under article 79(6) of the proposed regulation, a fine of a maximum of 2% of the annual worldwide turnover of the company can be imposed in this situation.

Tips & Tricks

Preparatory measures:

- Create an e-Discovery team (legal, IT, HR) and a document control team (lawyers, paralegals).
- In advance, enter into an agreement with a provider of e-Discovery software and services.
- Set the procedures to be followed in the case of e-Discovery or an investigation.

For e-Discovery and investigations:

- As soon as it is evident that a discovery request will be submitted, the legal department should identify the employees involved (the custodians).
- With the assistance of an e-Discovery provider, secure the e-mail inboxes and files of the custodians and store these on a separate server with strict access protocols.
- The provider must separate personal e-mails from business e-mails (using specialised software and a specific thesaurus).
- Have the document control team carry out manual checks of personal e-mails to see if they are relevant to the procedure.
- Have the provider select the other documents relevant to the case.
- Separate privileged information (lawyer - client correspondence).
- Have the document team manually check the remaining documents; business confidential and privacy-sensitive information will be redacted (blacked out).
- A transfer contract will be entered into with the recipient in the United States; this contract will be based on the standard contract clauses from the European Commission.
- Report the processing to the CBP.
- Inform the employees and third parties involved. (In certain circumstances, this may be done afterwards.)

SOURCES OF EUROPEAN AND DUTCH PRIVACY LAW

European law

Privacy Directive. Directive 95/46/EC of the European Parliament and of 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, OJ L No. L 281 of 23/11/1995 pages 0031 - 0050 (Privacy Directive).

Online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

1995 directive providing for privacy protection in the EU and implemented in all member states.

e-Privacy Directive. 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 and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

Online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

2009 directive providing for privacy protection in the context of the internet, among other things requiring consent for the placement of cookies on computers, smartphones, iPads, etc. and for accessing the information stored in the cookie.

Data Transfer Contract Decision. Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.

Online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0915:EN:NOT

2004 decision providing the standard contractual clauses to be used for the transfer of personal data to countries not having an adequate level of protection.

Proposal for the General Data Protection Regulation. 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), 25/1/2012, COM(2012) 11 final.

Online: http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf.

2012 proposal expected to replace the 1995 Privacy Directive and the 27 implementation laws with an EU-wide regime in 2014 or 2015.

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))

Online: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

Report by the rapporteur on the 2012 proposal for the General Data Protection Regulation, containing inter alia amendments proposed by a number of European parliamentary committees

Dutch law

Dutch Data Protection Act. Personal Data Protection Act, Bulletin of Acts and Decrees 2000, 302.

Online: http://www.dutchdpa.nl/Pages/en_wetten_wbp.aspx

2000 act implementing the 1995 Privacy Directive in the Netherlands.

e-Privacy Amendments. Act of 10 May 2012 to amend the Telecommunications Act for the implementation of the revised telecommunication guidelines, Bulletin of Acts and Decrees 2012, 235.

Online: June 2012 English version of entire Telecommunications Act available here: www.government.nl

2012 act implementing the 2009 e-Privacy Directive, including provisions dealing with cookies, spam and data reach notification requirements.

Whistleblower Committee Decision. Decision of 27 September 2011 to establish the Committee for the Whistleblower Advisory and Referral Point (Temporary Decision on the Committee for the Whistleblower Advisory and Referral Point) and explanatory memorandum, Bulletin of Acts and Decrees 2011, 427.

Decision in which the Dutch government established an independent agency to advise on and support potential and actual whistleblowers.

Dutch Corporate Governance Code. Dutch Corporate Governance Code, Government Gazette 18499 dated 3 December 2009, established by the Decree of 10 December 2009, Bulletin of Acts and Decrees. 545.

Online: https://docs.google.com/viewer?url=http://www.mccg.nl/download/?id%3D606

The 2009 corporate governance code for the business community, introduced by the government on the basis of the recommendations of the Frijns Committee.

Whistleblower Protection Bill. Legislative proposal made by the Dutch MPs Van Raak, Heijnen, Schouw, Van Gent, Ortega-Martijn and Ouwehand, concerning the establishment of a Whistleblower Office (Whistleblower Protection Act), with explanatory memorandum. Parliamentary Documents II 2012/13, 33 258 1 to 3.

Recommendations of the Council of State of 9 November 2012 (in Dutch only) are online: http://www.raadvanstate.nl/adviezen/zoeken_in_adviezen/zoekresultaat/?advicepub_id=10599.

Bill to improve the protection of and support for whistleblowers, e.g. by involving the National Ombudsman in reporting and investigation and by establishing a support fund.

Photgraphed Crimes Bill. Bill for an amendment to the Data Protection Act and other laws in connection with the expansion of the possibility of using camera images of criminal acts to support law enforcement and the introduction of a notification requirement in the case of breaches to personal data security measures (Amendment of the Data Protection Act concerning the use of camera images and the notification requirement for data breaches). Found at

Online (in Dutch only): http://www.internetconsultatie.nl/camerabeelden.

Bill to amend the Data Protection Act, introducing a general notification requirement for data breaches. To be submitted to the Tweede Kamer.

HOUTHOFF BURUMA PRIVACY TEAM

This publication was written by the Houthoff Buruma Privacy Team.

Houthoff Buruma is one of the largest law firms in the Netherlands. Its privacy team has many years of experience in advising on privacy law matters and assisting clients to ensure that their corporate policy and practice complies with European and Dutch privacy legislation. The team conducts regular privacy audits for clients in a compliance context. It provides guidance to clients in various sectors (including e-business, automotive, insurance and retail) on the use of customer data for customer activities. The team has specific expertise in helping healthcare institutions handle patient data and electronic patient files.

The team regularly advises on the privacy aspects of e-Discovery and regulatory investigations, both Dutch and international. The team is currently involved in a range of privacy matters, including the new cookie rules, central HR and career databases, document retention policies, whistleblower procedures, data breach notification, internet and e-mail codes of conduct for employees, and the transfer of data to the United States and other non-EEA countries. The team members are also involved in advising the buyers or sellers in major transactions.

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

Annemarie Bloemen
Senior associate at Houthoff Buruma, Dutch lawyer specialising in privacy and e-business
T +31(20)605 6554 | a.bloemen@houthoff.com

Franciska Voorberg
Associate at Houthoff Buruma, Dutch lawyer specialising in e-business and privacy
T +31(20)605 6956 | f.voorberg@houthoff.com

HOUTHOFF BURUMA OFFICES

Amsterdam
P.O. Box 75505
1070 AM Amsterdam
Gustav Mahlerplein 50
1082 MA Amsterdam
The Netherlands
T +31 (0)20 605 60 00

Rotterdam
P.O. Box 1507
3000 BM Rotterdam
Weena 355
3013 AL Rotterdam
The Netherlands
T +31 (0)10 217 20 00

Brussels
Keizerslaan 5
1000 Brussels
Belgium
T +32 (0)2 507 98 00

London
33 Sun Street
London EC2M 2PY
United Kingdom
T +44 (0)20 7422 5050

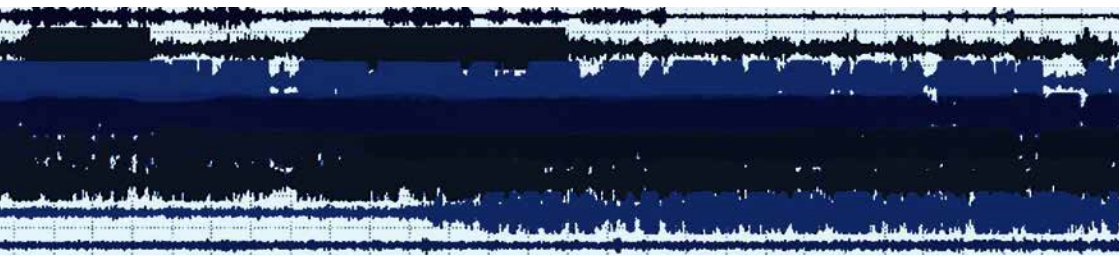
New York
120 West 45th Street, 19th floor
New York, NY 10036
USA
T +1 212 403 6701

www.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.



WWW.HOUTHOFF.COM