

## 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.<sup>1</sup>

In the context of civil litigation, Rule 26 of the US Federal Rules of Civil Procedure (FRCP)<sup>2</sup> 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

---

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

---

<sup>1</sup> Rotterdam Court, 8 August 2012, JBPR 2012 vol. 5, with note by R.B. van Hees and P.J. van der Korst.

<sup>2</sup> 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; whereas 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),<sup>3</sup> the Code of Federal Regulations,<sup>4</sup> the Foreign Asset Control Regulations,<sup>5</sup> the Sherman Antitrust Act<sup>6</sup> and the Sarbanes-Oxley Act (SOX).<sup>7</sup>

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.

---

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

<sup>4</sup> Several laws forbid the export of military goods and goods that can be used for military purposes.

<sup>5</sup> 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>.

<sup>6</sup> 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>.

<sup>7</sup> 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).<sup>8</sup> According to the legal definition of “personal data”, personal data 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.<sup>9</sup> Furthermore, if an individual is identifiable from the context of the information, or by the combination of information, this too may constitute personal data.<sup>10</sup> 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.

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

---

<sup>8</sup> Data Protection Act, Bulletin of Acts and Decrees 2000, 302.

<sup>9</sup> 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](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf).

<sup>10</sup> 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.

---

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

---

of this, there is a tendency to ignore the Act with this conflict arises.<sup>11</sup> 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<sup>12</sup> 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.<sup>13</sup> 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

---

<sup>11</sup> 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.

<sup>12</sup> 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](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf).

<sup>13</sup> 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](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.<sup>14</sup> 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.<sup>15</sup>

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.<sup>16</sup> In response to this (the Albrecht Report published in January 2013), the rapporteur of the European Parliament proposed significantly limiting this basis.<sup>17</sup> 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.<sup>18</sup>

### 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).

---

<sup>14</sup> Article 29 Working Party, WP158, p 9.

<sup>15</sup> Article 29 Working Party, WP158, p 9.

<sup>16</sup> Proposed regulation, Article 6(1)(f)

<sup>17</sup> 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](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf).

<sup>18</sup> 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.

### 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

---

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

---

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.<sup>19</sup> The European Commission has identified countries considered to have an adequate level of protection.<sup>20</sup> 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".<sup>21</sup> 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<sup>22</sup> (or, for an investigation, the FCPA<sup>23</sup> 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

submitted.<sup>24</sup> 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*,<sup>25</sup> 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.<sup>26</sup> 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.<sup>27</sup> The argument that the procedures set out in the Hague Evidence Convention must be followed is usually not accepted by an American court.<sup>28</sup> Under the Hague Evidence Convention, the gathering of

---

<sup>24</sup> *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.

<sup>25</sup> *Société Nationale Industrielle Aerospatiale v. U.S.*, District Court for the Southern District of Iowa, 482 U.S. 522 (1987).

<sup>26</sup> *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.Y. 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).

<sup>27</sup> *Convention on the Taking of Evidence Abroad in Civil or Commercial Matters*, The Hague, 18 March 1970 (Treaty Series 1979, 38).

<sup>28</sup> *Société Nationale Industrielle Aerospatiale v. U.S.*, District Court for the Southern District of Iowa, 482 U.S. 522 (1987).

---

<sup>19</sup> Dutch Data Protection Act, art 77.

<sup>20</sup> Andorra, Argentina, Australia, Canada, Switzerland, Israel, Faroe Islands, Guernsey and Isle of Man (on 1 Feb 2013).

<sup>21</sup> US-European Safe Harbor framework. Found at <http://export.gov/safeharbor>.

<sup>22</sup> See footnote 1.

<sup>23</sup> See footnote 2.

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.<sup>29</sup> 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.<sup>30</sup> 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).

---

<sup>29</sup> See, for example, *In re Vitamins Antitrust Litigation*, 2001 US Dist. Lexis 8904.

<sup>30</sup> 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).<sup>31</sup> 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).<sup>32</sup> 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

---

<sup>31</sup> 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.

<sup>32</sup> 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.)

**The members of the Houthoff Buruma Privacy Team:**

Wolter Wefers Bettink

Partner at Houthoff Buruma, Dutch lawyer specialising in IP and IT litigation, privacy and e-business  
T +31(20)605 6167 | w.bettink@houthoff.com

Thomas de Weerd

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

Copyright © 2013 Houthoff Buruma

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

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