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 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

[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.

[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.

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.