HOUTHOFF BURUMA

December 2015

News Update Privacy and Data Protection

New data breach notification act in effect from January 1, 2016

On January 1, 2016, the Act on Data Breach Notifications (Meldplicht Datalekken) ("Act"), will come into force. The Act introduces an obligation for data controllers virtually all organizations in the public and private sector) to report any data breaches that (are likely to) have serious adverse consequences for the protection of personal data into the Dutch Data Protection Act.

The Act includes an obligation to notify such data breaches to the Data Protection Authority ("DPA"). In addition, the data controller is also obliged to report a data breach to the involved data subjects (for instance customers, patients) in the event the privacy of these data subjects is adversely affected as a result of this data breach.

Failure to (timely) notify the DPA, and if required the involved data subjects, may lead to substantial fines up of to EUR 810,000 or 10% of the data controller's net annual turnover.

Background

The Act anticipates the expected coming into force of the draft European General Data Protection Regulation ("Regulation)", as this Regulation also contains obligations to report data breaches to the supervisory authorities and data subjects under similar conditions. Moreover, the Act aims to have preventive and repressive effects, by restoring overall trust in personal data use and limiting the adverse effects of data breaches.

Who, when, what and how to report

The obligation to report data breaches applies to organizations in both the private and public sectors that qualify as a "data controller" within the meaning of the Dutch Data Protection Act.

Not all data breaches are subject to the reporting obligation. The obligation to report data breaches, as laid down in the Act, pertains to *personal* data breaches, and to breaches that have, or are likely to have, serious adverse consequences for the protection of personal data. The explanatory memorandum to the Act and the (draft) guidelines on data breaches provided by the DPA stipulate

several examples of data breaches, such as stolen laptops, lost USB-sticks, hacking attacks or malware infections.

After discovery of a data breach, the data controller is obliged to notify the DPA immediately, though ultimately within two (2) business days after discovery thereof. In case the data controller uses a data processor, the latter should be obliged to immediately report a data breach to the data controller to enable a timely notification to the DPA. Data processing agreements should include this obligation for the data processor and are likely to require amendments.

The notification should at least include information regarding:

- the nature of the data breach;
- the identity of the parties with which additional information on the data breach can be obtained;
- suggested measures to mitigate the adverse consequences of the data breach;
- the established and expected consequences of the data breach for the processing of personal data, including suggested measures or measures the data controller has taken to remedy these consequences.

Data breaches can be reported to the DPA by submitting a web form (to be made available by the DPA), via the DPA's website or by fax.

In the event the data breach has, or is likely to have adverse consequences for the data subject, the data subject is required to be notified as well. Data subjects are to be informed in a manner that ensures an appropriate and accurate provision of information. The Act does provide an exception to the notification obligation towards the data subject. Appropriate technological protection measures (such as cryptography or remote wiping) may release a data controller from its notification obligation towards the data subject, provided that the data is intelligible for unauthorized persons.

Data breach register

The Act further introduces an obligation for data controllers to maintain an internal data breach register, in which the data breaches are recorded.

Sanctions

Failure to comply with the new data breach legislation, may lead to administrative fines imposed by the DPA amounting to EUR 810,000 or 10% of the net annual turnover of the data controller.

December 2015

News Update Privacy and Data Protection

Practical consequences

As of January 1, 2016, data controllers should:

(i) ensure that your organization's data security measures and policies are effective and up to date;
(ii) prepare a data breach notification protocol; and
(iii) verify that data processor agreements include appropriate data breach clauses and obligations for the data processor.

Please contact Thomas de Weerd and Jan Brölmann from Houthoff Buruma's privacy team for any questions regarding the data breach notification obligations. Or visit our website.

Contact

Thomas de Weerd
Partner
T +31206056985
M +31651659208
E t.de.weerd@houthoff.com
Amsterdam

Jan Brölmann
Lawyer
T +31206056594
M +31647043567
E j.brolmann@houthoff.com
Amsterdam

I would like to subscribe to the News Update Privacy and Data Protection