GDPR Update: Data Breaches and Notifications

September 22, 2017

Introduction

Under the GDPR, data security plays a prominent role and the GDPR imposes strict obligations on data controllers and data processors regarding security. While the Dutch Data Protection Act (DDPA) already includes a data breach notification regime, the GDPR introduces new notification obligations for various other EU countries.

The GDPR data breach notification regime differs on various aspects from the current data breach notification regime under the DDPA. This ninth GDPR update focusses on the obligation to notify data breaches to the data protection supervisory authority and data subjects, and the differences with the notification obligations under the DDPA.

What are data breaches?

The GDPR contains a broad definition of a data breach: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

The definition of a data breach is therefore not limited to hackers accessing the IT systems. It also includes lost or stolen smartphones, laptops or USB-sticks, malware infections and lost data (e.g. when data is accidentally deleted and there is no back-up available).

Notification to supervisory authority

Data breaches, if not addressed in an appropriate and timely manner, may result in damages to data subjects, including discrimination, identity theft, fraud, financial loss, damage to reputation, loss of confidentiality, etcetera.

Therefore, the data controller should notify the data breach to the competent supervisory authority without undue delay and, where feasible, no later than 72 hours after discovery of the data breach. This enables the supervisory authority to assess the breach and determine if follow-up actions are required.

Notification is not required if the data breach is unlikely to result in a risk to the rights and freedoms of the data subjects. This criterion differs slightly from the criterion under the DDPA, where a data breach must be notified to the supervisory authority, if the breach leads to a considerable likelihood of serious adverse effects on the protection of personal data, or if it has serious adverse effects on the protection of personal data. Arguably, the GDPR criterion will give rise to the notification obligation more quickly.

Under the GDPR, the notification to the competent supervisory authority must include:

i. a description of the nature of the data breach, including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
ii. name and contact details of the data protection officer or other contact point where more information can be obtained;
iii. a description of the likely consequences of the data breach; and
iv. a description of the measures taken or proposed to be taken by the controller to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If the notification cannot be achieved within 72 hours after discovery, the data controller must also provide the reasons for the delay. In practice data controllers should work with a 72 hours deadline for notification and should therefore have adequate internal procedures in place to allow them to meet this deadline.

Notification to data subjects

In addition to the notification to the supervisory authority, data controllers are obliged to inform the affected data subjects about the data breach without undue delay, unless:

i. the breach is unlikely to result in a high risk to the rights and freedoms of the affected data subjects (either by its nature or because the data controller has taken adequate subsequent measures);
ii. appropriate technical and organisational measures had been implemented and these measures were applied to the affected personal data; or
iii. the notification would involve a disproportionate effort. In such a case, the data controller is obliged to inform the data subject by public communication or similar measure. In case the data controller can reach the data subjects via electronic means, e.g. via e-mail, then the controller should assume that the notification does not involve a disproportionate effort.

The criteria to notify the data subjects also slightly differ from the criteria under the DDPA. Under the DDPA, the data subjects must be notified if the data breach is likely to have adverse effects for their privacy, unless appropriate measures are taken that render the personal data incomprehensible or inaccessible to unauthorised persons. Consequently, the criteria to notify the data subjects appear to be less stringent under the GDPR, in the sense that there appears to be a higher threshold for notification.

The communication to the data subjects must describe in clear and plain language the nature of the data breach and must contain at least the same information as the notification to the supervisory authority (as listed above).

If the data controller has not (yet) notified the data subjects, the supervisory authority may require it to do so. Failure to comply may result in significant fines (see below).

Internal record of data breaches

Data controllers are obliged to document all data breaches, including relevant facts relating to the data breach, its effects and any remedial actions taken.

Data breach obligations for data processors

Under the GDPR, data processors are obliged to report a data breach to the data controller without undue delay after

becoming aware of the breach, allowing the data controller to take the necessary actions in a timely manner. It is advisable to make clear arrangements on when and how data processors notify the data controller. We would recommend that data controllers and data processors agree in the processor agreement that it is better to notify an incident that turns out not to be a data breach, than to not notify an incident that in hindsight should have been qualified as a data breach.

Fines

Failure to comply with the above obligations may result in fines up to € 10,000,000 or 2% of the total worldwide annual turnover, whichever is higher. Non-compliance with an order by the supervisory authority may result in fines up to € 20,000,000 or 4% of the total worldwide annual turnover, whichever is higher.

Practical recommendations and conclusion

Taking into account the limited time available for notifying the supervisory authority and the data subjects of a data breach, organisations would do well to implement a data breach response plan setting out the actions to be taken internally in the event of a data breach, including key contacts (both internal and external), checklists and follow-up measures. Worldwide organisations should also consider setting up regional/local data breach response teams (which may include external experts such as outside counsel, IT forensics and PR experts).

Please click here to subscribe to our monthly updates on the GDPR.

Overview of subjects

January 2017	Territorial scope of the GDPR(Dutch)
February 2017	The Concept of Consent
March 2017	Sensitive Data
April 2017	Accountability, Privacy by Design and Privacy by Default
May 2017	Rights of Data Subjects (information notices)
June 2017	Rights of Data Subjects (access, rectification and portability)
July2017	Rights of Data Subjects (erasure, restriction, objectand automated individual decision-making)
August 2017	Data Processors
September 2017	Data Breaches and Notifications
October 2017	Data Protection Officers
November 2017	Transfer of Personal Data (outside the EEA)
December 2017	Regulators (competence, tasks and powers)
January 2018	One Stop Shop
February 2018	Sanctions
March 2018	Processing of Personal Data in Employment Context
April 2018	Profiling and Retail
May 2018	Overview

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com