14 September 2015

LOYENS & LOEFF

Privacy Newsletter

Klik hier voor de Nederlandse versie

Data breach notification

Introduction

A lost, unprotected USB-stick, a stolen laptop or the hack of a dating site. As of 1 January 2016, all security incidents that unintentionally result in the disclosure of personal data to third parties, will have to be reported to the Dutch Data Protection Authority and, in certain cases, even to the person whose personal data has been disclosed. Failing to report such an incident to the aforesaid parties may lead to fines of up to EUR 810,000 or 10% of the company's net annual turnover.

The Data Breach (Notification Obligation) Act

The "Data Breach (Notification Obligation) Act and the extension of the power to impose fines" comes into force on 1 January 2016. This Act will insert into the Dutch Data Protection Act an obligation to report a data security breach. The introduction of this obligation anticipates the European General Data Protection Regulation, which is expected to introduce a similar obligation as of 2018. Furthermore, the violation of various provisions that are included in the Dutch Data Protection Act will be fined more heavily. The number of provisions in the Dutch Data Protection Act for which an administrative fine can be imposed will also be increased.

What and when to notify?

The obligation to notify a data security breach is closely connected to the obligation to implement adequate technical and organizational security measures to the protect personal data against loss and any form of unlawful processing (as specified in article 13 of the Dutch Data Protection Act). When a breach of the required security measures is discovered that is associated with *possible severe negative consequences for the protection of personal data*, the data controller (the party that determines the purpose and means of the data processing) should immediately report this to the Dutch Data Protection Authority (as from 1 January 2016 the "Personal Data Authority" (**Authority**)). A security breach can take many forms: from a person entering a building and accessing or even taking personal data, to the more infamous example of a hacker. A lost phone, laptop or USB-stick can also be regarded as a breach of the required security measures.

If it is likely that a security breach will *negatively affect the privacy of the data subject* (i.e. the person whose personal data was disclosed), that individual should be notified of the data breach immediately. As a general rule, the decision whether or not to notify the data subject is up to the data controller. However, if the Authority disagrees with the decision of the data controller *not* to notify the data subjects, the Authority can force the data controller to notify them nonetheless.

The obligation to notify the data subjects does not apply when the data controller has taken technical security measures that make personal data either unclear or inaccessible to anyone who does not possess the right to access the data. For example, if a lost USB-stick is encrypted, the data controller will not be obliged to notify the persons whose personal data was saved on the USB-stick. Furthermore, financial institutions that are subjected to the Dutch Financial Institutions Act are excluded from the obligation to notify the data subjects: these institutions will only have to notify the Authority.

Who?

The parties that are obligated to notify a personal data breach are organisations in both the private and public sectors that qualify as a 'data controller' under the Dutch Data Protection Act.

How to report?

The notification of a personal data breach needs to include the following information:

- the nature of the data breach;
- the authorities where additional information about the data breach can be obtained;
- recommendations on how to limit the consequences of the data breach;
- a description of the probable consequences of the data breach for the processing of personal data and the measures that the data controller has taken or proposes to take in order to remedy these consequences.

The data subjects should be notified in a manner that guarantees sufficient and accurate provision of information.

Furthermore, the data controller is required to keep a record of all personal data breaches.

Penalties

At this moment, the maximum administrative fine for non-compliance with the Dutch Data Protection Act is EUR 4,500, and the Authority has limited power to impose a fine. However, this situation will change as of 1 January 2016. From that moment onwards, the Authority will be able to impose fines for non-compliance with a substantial amount of provisions of the Dutch Data Protection Act. Also, the maximum amount of the possible fine will increase substantially: non-compliance with the obligation to notify can result in a fine up to a maximum of EUR 810,000 or even 10% of the annual net turnover of a company, per violation. The Authority is generally required to give a binding instruction before imposing a fine.

What does this mean for you?

When a data security breach is discovered, your organisation will have to notify this immediately to the Authority and, in certain situation, to the data subjects concerned. As the notification has to be done immediately (as soon as reasonably possible), it will be too late to draw up a plan of action at the moment that a data security breach is discovered. Therefore, as from 1 January 2016, each organization needs to have an action plan for the unlikely event of a data breach.

Questions?

For more information, please contact:

Kim Lucassen

kim.lucassen@loyensloeff.com

+31 10 224 6416

Joanne Zaaijer

joanne.zaaijer@loyensloeff.com

+31 10 224 6164

Meldplicht datalekken

Inleiding

Een verloren, onbeveiligde, USB-stick, een gestolen laptop of een hack van een datingwebsite. Vanaf 1 januari 2016 moeten incidenten waarbij onbedoeld persoonsgegevens voor derden toegankelijk zijn geworden, worden gemeld aan het College bescherming persoonsgegevens, maar in sommige gevallen ook aan degene wiens gegevens het betreft. Wordt een dergelijke melding niet of niet tijdig gedaan, dan kunnen er forse boetes volgen.

Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp

Op 1 januari 2016 treedt de “Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp” in werking. De wet introduceert een meldplicht voor datalekken in de Wet bescherming persoonsgegevens (**Wbp**). De introductie van deze meldplicht in de Wbp loopt daarmee vooruit op de Europese Algemene Verordening Gegevensbescherming waarin naar verwachting met ingang van 2018 een vergelijkbare verplichting zal worden opgenomen.

Daarnaast zullen met ingang van 1 januari 2016 fors hogere boetes gelden voor overtreding van diverse bepalingen van de Wbp. Ook het aantal bepalingen uit de Wbp dat bestraft kan worden met een boete, neemt sterk toe.

Wat en wanneer melden?

De meldplicht hangt nauw samen met de verplichting van artikel 13 Wbp om voldoende organisatorische en technische beveiligingsmaatregelen te nemen. Op het moment dat een inbreuk op de vereiste beveiligingsmaatregelen wordt geconstateerd die *potentieel ernstige nadelige gevolgen heeft* voor de bescherming van persoonsgegevens, dan moet de verantwoordelijke (degene die het doel en de middelen van een gegevensverwerking bepaalt) onverwijld het College bescherming persoonsgegevens (vanaf 1 januari 2016 “Autoriteit persoonsgegevens” (**Autoriteit**)) inlichten. Een dergelijke inbreuk kan allerlei vormen aannemen: het kan gaan om iemand die zich feitelijk toegang heeft verschaft tot een gebouw en mogelijk persoonsgegevens heeft ingezien of meegenomen, tot het meer aansprekende voorbeeld van een hacker. Maar ook het verlies van een telefoon, laptop of USB-stick kan een inbreuk op de beveiliging zijn.

Als die inbreuk op de beveiliging daarnaast ook nog *waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene* (degene wiens gegevens het betreft), zal ook deze betrokkene onverwijld moeten worden ingelicht. De afweging of daarvan sprake is, is in beginsel aan de verantwoordelijke zelf, maar als deze besluit dat melding aan de betrokkene niet nodig is, kan de Autoriteit de verantwoordelijke vervolgens alsnog verplichten om de betrokkenen in te lichten.

De verplichting om de betrokkene te informeren geldt niet indien de verantwoordelijke technische beveiligingsmaatregelen heeft genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens. Dus bijvoorbeeld in geval van verlies van een USB-stick die is beveiligd door encryptie, hoeft de verantwoordelijke de personen wiens gegevens op die USB-stick staan, daarvan niet op de hoogte te stellen. Daarnaast zijn financiële ondernemingen als bedoeld in de Wet op het financieel toezicht uitgezonderd van de meldingsplicht aan de betrokkene: financiële ondernemingen hoeven alleen een melding aan de Autoriteit te doen.

Wie?

De meldplicht geldt zowel voor organisaties in de private als in de publieke sector die als verantwoordelijke in de zin van de Wbp kwalificeren.

Hoe melden?

De melding aan de Autoriteit dient in ieder geval de volgende gegevens te bevatten:

- Aard van de inbreuk;
- Waar meer informatie over de inbreuk kan worden verkregen;
- Aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- Beschrijving van de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

Voor de kennisgeving aan de betrokkene geldt dat deze op zodanige wijze moet worden gedaan, dat een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.

De verantwoordelijke is daarnaast verplicht om een overzicht bij te houden van alle inbreuken.

Sancties

Waar de maximale bestuurlijke boete voor overtreding van de Wbp op dit moment nog EUR 4.500 bedraagt en het CBP maar zeer beperkt de mogelijkheid heeft een bestuurlijke boete op te leggen (alleen met betrekking tot de meldingsplicht), neemt deze bevoegdheid met ingang van 1 januari 2016 exponentieel toe. Vanaf dat moment zal de Autoriteit ook bevoegd zijn om een bestuurlijke boete op te leggen voor overtreding van een groot aantal bepalingen van de Wbp. Ook de hoogte van de boete is fors gestegen: zo kan niet naleving van de meldplicht datalekken resulteren in een boete van maar liefst EUR 810.000 of 10% van de jaaromzet van een onderneming per overtreding. Het is in de regel wel vereist dat de Autoriteit eerst een bindende aanwijzing geeft.

Wat betekent dit voor u?

Bij constatering van een inbreuk moet uw organisatie daarvan onverwijld mededeling doen. Aangezien onder “onverwijld” zo snel als redelijkerwijs mogelijk moet worden verstaan, is het op het moment dat er een datalek wordt geconstateerd, in ieder geval te laat om nog een draaiboek te maken. Vanaf 1 januari 2016 zal iedere organisatie dus een plan van aanpak moeten hebben klaarliggen voor het geval zich onverhoopt een inbreuk op de beveiliging voordoet.

Vragen?

Voor vragen kunt u contact opnemen met:

Kim Lucassen
kim.lucassen@loyensloeff.com
+31 10 224 6416

Joanne Zaaijer
joanne.zaaijer@loyensloeff.com
+31 10 224 6164

Disclaimer