Netherlands

New Notification Obligations and Fines Under the Dutch Data Protection Act

*Sarah Johanna Eskens**

I. Introduction

As of 1 January 2016, the Dutch Data Protection Act ('the Act') has changed considerably. Most importantly, the revised Act contains a security breach notification obligation, expands the power of the Dutch data protection authority ('the Dutch DPA') to impose fines for violation of the Act, and renames the Authority. This report gives some background on the changes and sets out the new provisions in more detail.

II. Background

In June 2013, the Dutch government submitted a legislative proposal to include a security breach notification obligation in the Dutch Data Protection Act. The proposal responded to a large number of incidents in the Netherlands. These incidents involved breaches of website security in which personal data were released, with adverse effects on the privacy of the persons concerned. In a couple of cases these were very serious breaches, in terms of the amount of personal data released and the nature of the data. Therefore, the purpose of the new notification obligation is to prevent security breaches and, if they occur nonetheless, to limit the consequences for the persons concerned. As such, the notification obligation should contribute to the preservation and recovery of trust in the handling of personal data.

The legislative proposal suggested empowering the Dutch DPA to impose an administrative fine for violations of the security breach notification obligation, but later in the legislative process such powers were further expanded.

III. The New Security Breach Notification Obligation

1. A Security Breach

A new Article 34a of the Act obliges controllers to notify, under certain circumstances, the Dutch DPA and the data subject of a security breach. The Act links the notion of 'security breach' to the existing requirement that data controllers implement appropriate technical and organizational security measures to protect personal data against *loss* or *any unlawful form of processing*.[1] Examples of a security breach are the hack of an ICT system, theft of a laptop, loss of a USB-stick, or a malware infection.

2. Notification to the Dutch DPA

The revised Act requires that data controllers notify, without delay, the Dutch DPA of a security breach that results in a *considerable* chance to *seriously adversely affect* or actually *seriously adversely affects* the *protection of personal data*.[2] Given the notion of a 'security breach', this provision implies that organizations should only notify the Dutch DPA where security measures did not function properly, and the personal data either have been exposed to a considerable chance of loss or any unlawful form of processing, or are actually lost or unlawfully processed. The Explanatory Memorandum to the legislative proposal explains that this qualification intends to prevent unnecessary notifications.

* Sarah Johanna Eskens is a PhD candidate at the Institute for Information Law (IViR), University of Amsterdam. For correspondence: <s.j.eskens@uva.nl>.

1 art 31a(1) in conjunction with art 13 Dutch Data Protection Act.

2 art 31a(1) Dutch Data Protection Act..

The Act requires that the notification to the Dutch DPA (and the data subject; see below) in any case comprises the nature of the breach, the bodies where more information about the breach can be obtained and the recommended measures to mitigate the adverse effects of the breach.[3] In addition, the Act requires that the notification to the authority includes a description of the found and probable effects of the breach for the processing of personal data, as well as the measures that the controller has taken or proposes to take in order to remedy these effects.[4]

3. Notification to the Data Subject

Next to notification to the Dutch DPA, the revised Act requires that data controllers notify, without delay, the data subject of a security breach, if the breach is *likely* to *unfavourably affect* his or her *privacy*.[5]

Similarly to the notification to the Authority, the Act requires that the notification to the data subject in any case comprises the nature of the breach, the bodies with more information, and the recommended measures to mitigate the adverse effects of the breach.[6] The Explanatory Memorandum to the Act clarifies that the recommended measures should focus on the data subject, in the sense that the controller should recommend the data subject what to do on their own to mitigate the damage of the breach, such as changing username and password.

The Act stipulates that the data subject should be notified in such a manner that, taking into account the nature of the breach, the found and actual effects thereof for the processing of personal data, the group of persons concerned and the costs of implementation, a sufficient and careful provision of information is guaranteed.[7] According to the Explanatory Memorandum, this means the controller may inform a small group of data subjects personally, whereas a newspaper ad is probably more appropriate in case of a large number of persons concerned.

4. Exemptions from the Notification Obligation

The revised Act states notification to the data subject is not required where the controller has implemented appropriate technical safeguards that rendered the personal data unintelligible or inaccessible to any person who is not authorized to learn of the data (for example, encryption).[8] Still, in case the controller does not notify the data subject, the Act empowers the Dutch DPA to demand that the controller notify the data subject, if the Authority is of the view that the breach likely unfavourably affects the privacy of the person concerned.

Furthermore, the Act states that notification is not required if the controller has already notified the Dutch DPA and eventually the data subject of the security breach in his capacity as a provider of a public electronic communication service.[9]

5. Policy Rules of the Dutch DPA

Organisations should determine themselves whether an actual security breach falls within the scope of the notification obligation. The Dutch DPA has published policy rules on the new obligation to help organisations determine whether they should notify an actual breach. Even earlier, the Authority published guidelines on what constitute 'appropriate' security measures within the meaning of the Act.

IV. Fines for Violations of the Act

A renewed Article 66 of the Act significantly expands the power of the Dutch DPA to impose fines for violations of the Act. Before this, the Authority could impose an administrative fine not exceeding € 4,500 for not notifying the supervisory authority of processing operations or for noncompliance with the content requirements for such a notification.[10]

3 art 34a(3) Dutch Data Protection Act.

4 art 34a(4) Dutch Data Protection Act.

5 art 34a(2) Dutch Data Protection Act.

6 art 34a(3) Dutch Data Protection Act.

7 art 34a(5) Dutch Data Protection Act.

8 art 34a(6) Dutch Data Protection Act.

9 art 34a(9) Dutch Data Protection Act in conjunction with arts 11.3a(1) and 11.3a(2) Dutch Telecommunications Act. The legislative proposal for the Dutch Data Protection Act also changed the concerned provision of the Dutch Telecommunications Act: originally, providers of public electronic communication services had to notify the Dutch Authority for Consumers & Markets of a security breach.

10 arts 27 and 28 Dutch Data Protection Act.

The Act now empowers the Dutch DPA to impose an *administrative fine not exceeding €820,000* or a *fine not exceeding 10% of an organisation's annual turnover* for a violation of most of the provisions of the Dutch Data Protection Act.[11] However, the Act specifies that the Authority may impose such a fine not before it has issued a binding instruction with regard to the violation.[12] Yet, if the violation was intentional or the result of serious culpable negligence, the Authority may impose a fine without first issuing such a binding instruction.[13]

As stated in the introduction, the legislative proposal only empowered the Dutch DPA to impose an administrative fine for violation of the notification obligation. Later in the legislative process, an amendment expanded the power to impose fines to more provisions of the Act and increased the maximum amount of the fine. This amendment also introduced the requirement that the authority should first issue a binding instruction before imposing a fine, unless the violation was intentional. After a negative response by the Dutch DPA, another amendment added that a binding instruction is neither required if the violation is the result of serious culpable negligence.

V. A New Name

Finally, the revised Act provides that the Dutch DPA, previously called '*College Bescherming Persoonsgegevens*', will now be called '*Autoriteit Persoonsgegevens*' – at least in the daily course of affairs.[14] In a press release, Jacob Kohnstamm, the Chairman of the Authority, declared that the new position of a strict enforcing body called for an 'Authority' (instead of the more general 'college', which means 'board').

11 art 66(2) Dutch Data Protection Act in conjunction with arts 23(4) and 23(7) Dutch Penal Code.

12 art 66(3) Dutch Data Protection Act.

13 art 66(4) Dutch Data Protection Act.

14 art 51(4) Dutch Data Protection Act.