CLIFFORD
CHANCE

Client briefing December 2015

New Dutch security breach notification rules: are you prepared?

As of 1 January 2016, new rules will enter into force under the Dutch Data Protection Act. Data controllers will be obliged to notify the Dutch Data Protection Authority, and, in certain cases, also data subjects of serious security breaches impacting personal data. In addition, the Dutch Data Protection Authority's powers of enforcement will be significantly enhanced, allowing for the imposition of fines for data protection violations up to EUR 820,000 or even 10% of a company's annual net turnover per violation. At the same time, the enforcement of the Data Protection Act is said to be intensified, all of which makes compliance a risk control topic to be addressed at a board room level. This briefing discusses the new rules and the preparatory actions to be taken.

Context and guidelines

The new breach notification requirements under the Dutch Data Protection Act ("DPA") precede similar requirements that will apply under the proposed EU General Data Protection Regulation, which is expected to enter into force no sooner than 2018. The new breach notification rules under the DPA sit along existing security breach notification duties, such as those imposed under the Dutch Telecommunications Act (*Telecommunicatiewet*) and the Dutch Act on Financial Supervision (*Wet op het Financieel Toezicht*).

In addition to the new DPA rules, which specifically concern security breaches involving personal data, more general security breach notification duties are in the make with respect to breaches of network and information security in sectors which are considered to involve critical infrastructures (eg the energy, telecoms, financial and transportation sectors). A new Act on Cyber Security notification duties (*Wet gegevensverwerking en meldplicht cybersecurity*) is anticipated, which has currently been published in draft form for public consultation and which anticipates the proposed EU Directive on Network and Information Security.

Key issues

What's new

- Duty to notify security breaches without delay
- Fines of up to EUR 820,000 or 10% of annual turnover

How does this affect organisations

- Update compliance policies and procedures
- Create a security breach response plan and incident response team
- Review and amend contracts with third parties

The Dutch Data Protection Authority ("DP Authority") has published policy rules regarding the application of the new breach notification rules ("Policy Rules"). The Policy Rules provide guidance for implementing appropriate measures, to explain when what has to be notified to whom and to clarify how the DP Authority will enforce the new rules. The Policy Rules build on existing guidelines with respect to breach notification duties in the electronic communications sector as published by the European Commission

(Regulation No 611/2013) and on an opinion (Opinion 03/2014) published by the Article 29 Working Party (a forum in which all EU Data Protection Authorities are represented).

Who is subject to the breach notification rules?

The new rules cut across all market sectors, affecting each and every organisation involved in the processing of personal data. Each data controller – the person or entity determining the purpose for the processing of personal data – in the Netherlands will be subject to the new breach notification rules. The data controller will also have to ensure that any third party data processors that it is using also comply with the new breach notification duties.

There are a few express exceptions for data controllers in specific sectors:

(a) **Providers of electronic communications services and networks:** these providers are already subject to separate security breach notification obligations under the Dutch Telecommunications Act. To the extent these providers have notified a security breach affecting personal data in accordance with those obligations, they need not also notify the breach under the new DPA rules. In an effort to streamline notification processes, the new DPA rules provide that security breaches have to be notified to the DP Authority instead of, as is currently the case, the Authority for Consumers and Markets (*Autoriteit Consument & Markt*).

(b) **Financial services organisations:** these organisations, as defined in the Dutch Act on Financial Supervision, are required to notify the DP Authority of security breaches affecting personal data, but are exempted from the obligation under the DPA to also notify the persons whose personal data is compromised. The rationale behind this exemption is to prevent mandatory public notifications having the effect of unnecessarily affecting the public's trust in the financial sector. Despite this exemption the general duty of care that applies to financial institutions may nevertheless in certain circumstances create a duty for the financial institution to inform affected customers of data breaches in consultation with the relevant financial supervisory authority.

Which breaches should be notified, and when and to whom?

Data controllers are generally required under the DPA to implement appropriate technical and organizational measures to protect personal data against loss and any form of unlawful processing. Not all breaches of these security measures have to be notified; only breaches that have (or create a significant chance of) serious adverse consequences for the protection of personal data. Whether or not a breach has or may have such serious adverse consequences is an assessment that the data controller will have to make, taking into account the (nature of the) affected personal data and the nature and scope of the breach. The Policy Rules contain examples of breaches that would have to be notified.

Breaches must be notified to the DP Authority "without delay" (*onverwijld*) and in any event no later than 72 hours after becoming aware of the data breach. If within this timeframe there is not enough clarity regarding the specifics of the security breach and to what extent personal data is affected, notification can be done based on the then current knowledge and the notification can be amended or even retracted once full clarity has been obtained.

If the breach is likely to have negative consequences for the privacy of individuals, the affected individuals should also be notified, unless technical measures such as encryption have been taken to render the compromised personal data illegible or inaccessible to unauthorised third parties. The DP Authority may also give the data controller a binding instruction to perform such notification. Not complying with the binding instruction could result in a fine of the highest category.

What needs to be notified?

The notification to the affected individuals and DP Authority should include the following information:

(i) the nature of the breach;

(ii) the contact details of the departments within the organisation that can provide further information about the breach;

(iii) recommended measures to mitigate the adverse consequences of the breach.

The notification to the DP Authority should in addition contain a description of the established and probable consequences of the breach for the processing of personal

data and the proposed measures or measures taken to remedy these consequences.

Data controllers will also have to maintain an overview of all security breaches that have occurred which have led to (a significant chance of) serious adverse consequences for the protection of personal data. This overview should contain the facts and details of the breach and the text of the notification given to the relevant individuals.

Enforcement and fines

As of 1 January 2016, the DP Authority will be authorised to impose substantially higher fines for violations of the DPA than is currently the case. These fines can be imposed for any breach of the DPA requirements, not only the new breach notification requirements. Fines have been divided into three categories depending on which specific provision of the DPA is breached:

(i) for minor breaches, fines can be imposed up to a maximum of EUR 20,250;

(ii) for more serious breaches, fines can run up to EUR 450,000; and

(iii) for the most serious and/or deliberate or repeated breaches, fines can run up to EUR 820,000 or 10% of the company's annual net turnover in the year preceding the breach.

Non-compliance with basic principles of the DPA, such as the requirement of a legitimate ground for the collection and processing of personal data or the prohibition to process sensitive personal data if no exemption applies, may result in companies forfeiting substantial fines. These fines can only be imposed after the DP Authority has issued a binding instruction to the company with which the company then fails to comply, unless the breach was committed intentionally or is the result of gross negligence.

Finally, the name of the DP Authority – currently, the *College bescherming persoonsgegevens* – will be changed to *Autoriteit Persoonsgegevens* (Personal Data Authority).

Recommendations

The introduction of the breach notification requirements requires organisations that process personal data and are subject to the DPA to review and where necessary amend their existing policies, procedures and potentially also the contracts they have in place with third parties that process personal data on their behalf.

Typical measures to ensure compliance include the following:

i) Reviewing and amending existing data security measures and data protection policies;

ii) Developing and implementing data breach notification procedures, including a registry to record breaches;

iii) Communicating the changes in policies and procedures internally and raising additional internal awareness of the risks of data breaches and the relevant procedures;

iv) Implementing a data breach response plan and related incident response team consisting of individuals with the appropriate expertise across the organisation up to the Board. Typically, an incident response team would consist of legal specialists, IT specialists, HR representatives, PR/Marketing specialists and a member of the Board;

v) Developing a communications plan and notification plan for (required) notifications to the DP Authority and affected individuals, and for possible communications to the general public and the media in the event of a serious data breach, taking into account potential liability exposure. In this context, it should be noted that the DPA does not contain a general immunity arrangement for companies that notify breaches, which entails that the information disclosed may be used against the company (either by the DP Authority or by affected individuals or organisations that are considering a claim);

vi) Identifying third party data processors and gathering sufficient information to determine if and to what extent these parties have in place the required policies and procedures to allow the organisation to meet its breach notification requirements;

vii) Where required, amending existing third party contracts to include breach notification obligations and identifying the categories of information that need to be shared with the organisation for it to meet the DPA breach notification requirements. In doing so, the aim should be to make the contracts "future proof" by also taking into account categories of information that will likely be part of breach notification requirements that will be introduced once the EU General Data Protection Regulation and the EU Network and Information Security Directive are adopted.

The data protection and cyber security experts of Clifford Chance can assist with any of the above measures. Please contact Nadia Jagusiak, Alvin Khodabaks or Jaap Tempelman for further information.

Contacts

Alvin Khodabaks
T: +31 20 7119 374
E: alvin.khodabaks@cliffordchance.com

Jaap Tempelman
T: +31 20 7119 192
E: jaap.tempelman@cliffordchance.com

Nadia Jagusiak
T: +31 20 7119 210
E: nadia.jagusiak@cliffordchance.com