Forewarned is forearmed: the learnings to take from the Dutch data security breach regime

January 2017

The sanction-heavy General Data Protection Regulation (the "**GDPR**"), with its mandatory breach notification regime, will be upon us in less than 18 months, and businesses are well advised to start preparing and implementing a plan now to ensure that they will be compliant. To assist with such plans, this briefing looks at what lessons can be learnt from the mandatory data security breach regime in the Netherlands, as well as practical learnings from previous incidents which we have advised on.

This briefing was first published in Privacy Laws & Business UK Report, Issue 89 (January 2017).

The GDPR's breach notification regime

The GDPR's mandatory breach notification regime deals with breaches of security leading to the loss, destruction, alteration, unauthorised access to or disclosure of personal data (referred to as "breaches" or "data breaches" in this briefing and as "personal data breaches" in the GDPR). Under the Data Protection Directive (95/46/EC), there is no mandatory notification requirement for data breaches. However, in the UK, the Information Commissioner's Office has advised data controllers to notify it of any serious data breaches they suffer and, at the same time, to consider whether a notification needs to be made to the affected individuals.

Under the GDPR, a data controller must:

- Notify the relevant DPA of a personal data breach without "undue delay" and, where feasible, within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the "rights and freedoms" of the relevant individuals. If a notification is not made within 72 hours, the data controller must provide the DPA with reasons for the delay; and

- Notify the relevant individuals of a personal data breach without "undue delay" where that breach is likely to result in a high risk to their "rights and freedoms" (except where the personal data concerned is unintelligible (e.g. through encryption), steps have been taken to ensure the relevant risk will not materialise or notification would involve disproportionate effort).

The GDPR takes us from a voluntary to a mandatory regime, requiring breaches that meet a certain threshold to be notified to the relevant data protection authority ("**DPA**") and in some cases to the affected individuals too.

A failure by a controller to notify the DPA or the affected individuals of a breach will not only result in DPA scrutiny and bad PR, but also in a fine of up to 2% of the controller's annual global turnover or €10 million (whichever is higher).

However, if a failure to notify is considered to be linked to the underlying data breach, the two combined may fall under the aggregate maximum cap of 4% of annual global turnover or €20 million (whichever is higher).

The Dutch data breach regime

In January 2016, the Netherlands introduced a mandatory breach notification regime. At our annual Data Protection and Privacy Forum in November, we held a series of roundtable sessions on the practical learnings businesses could derive from mandatory regimes such as the Dutch one.

Dutch requirements

- Notify the Dutch DPA of a personal data breach where there is a considerable chance of serious adverse effects on the privacy of individuals. Although the legislation does not specify a maximum time period for notification, the Dutch DPA's guidelines indicate that notification to the regulator should be made within 72 hours; and
- Notify data subjects where there is a considerable likelihood of the breach adversely affecting the privacy of the relevant individuals.

Whilst the wording in the Dutch legislation differs from the GDPR, in practice there are sufficient similarities between the two regimes for the Dutch experience to foreshadow the new GDPR requirements. This is due in part to guidance issued by the Dutch DPA on how the law should be applied, resulting in the threshold for breach notification being lower than expected.

The biggest challenges that had arisen for businesses under the Dutch regime were:

Timeframe for analysis

Identifying sufficient information for analysis within the timeframe was the key challenge. In some cases it had appeared that a notification would be required only for the IT team to identify at the last minute that the personal data which was thought to meet the threshold was not affected by the security breach. Likewise, ensuring that potential breaches are escalated swiftly rather than being viewed, for instance, simply as an IT issue has caused problems.

Uncertainty as to the threshold for notification

Given the risk based approach built into this threshold, it is hard to draw a clear line as to what is or is not notifiable.

In the early days of the Dutch regime, businesses had taken a cautious approach and most likely over reported. With the benefit of their experiences through 2016, businesses are now refining what they report.

Dealing with outsourced arrangements

Most businesses outsource at least some of their activities and this puts even greater pressure on obtaining the necessary (and accurate) information within the requisite period.

The information required for the notification

As a practical point, the Dutch form of notification requires very detailed information to be included. Businesses have learnt that it is best to notify the DPA without all the information initially as they can follow up with the missing items.

Under the GDPR the issues set out above are likely to arise for all data controllers. Some companies in the UK (i.e. those who are subject to mandatory notification under the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**")) have already experienced similar challenges to companies in the Netherlands, with the notification timings under PECR being tighter at 24 hours.

There are a number of learnings which can be taken from the Dutch experience and the PECR regime. The remainder of this briefing therefore looks at what actions businesses should take to put themselves in the best position possible by May 2018.

Practical learnings and preparation

Data security breach protocol

Businesses will need to have in place a robust data security breach protocol ("breach protocol") allowing them to respond swiftly to any breach they suffer, limit damage caused by that breach and comply with the GDPR's strict time constraints for notification.

However, there is no need to reinvent the wheel in devising such a protocol – existing processes or structures can be usefully leveraged or repurposed to accommodate data breaches. For example, companies with crisis management plans, business continuity plans or product recall plans may well be able to repurpose existing processes, which has the added benefit of the overall protocol appearing familiar.

Drawing on discussions at our Data Protection and Privacy Forum and the learnings from our experience in advising on data breach incidents, we consider the following elements to be of particular importance in any breach protocol:

- *A cross-disciplinary response team*. This team should include all appropriate departments such as the privacy team IT, PR, IR, Legal, Compliance, Internal Investigations and HR. This ensures that all relevant considerations are taken into account in formulating the response to any particular incident. We have seen too many incidents where some of the team have only been brought in at a late stage to the detriment of the overall response.

- *Means of communication*. Consider having an email group set up in advance so that all relevant members of the response team are notified and kept informed of any data breaches. This may already be set up for crisis management teams and could be used equally for breach incidents.

- *Internal escalation*. Given the tight notification deadline, it is also important that breaches are escalated up the chain to the appropriate people in a timely manner. Setting a low threshold for the internal reporting of breaches will help ensure all relevant incidents are considered for notification as well as helping businesses comply with the related GDPR requirement to keep a log of all personal data breaches.

- *Notification thresholds*. Businesses need to determine their thresholds for notification of breaches to DPAs and individuals. Data audits, which many companies are currently conducting, and data privacy impact assessments can provide useful information to help assess ahead of time which systems (if breached) or data (if exposed) are likely to require notification. Companies should also consider agreeing consistent standards for notification across sectors as this has proved useful in the Netherlands.

- *Decision making*. The breach protocol should be clear as to which individuals or functions have the authority to make the final call on whether a breach is notifiable; too many stakeholders may result in prolonged deliberations and resulting delays.

- *Stock exchange rules*. The breach protocol needs to cover whether the rules relating to the listing and trading of a company's shares require a formal announcement of the data breach. If so, this will typically drive the timing of the public response as the notification should not be made to the DPA until the stock exchange notification is made. In practice, therefore, the different announcements and notifications should be lined up to be made simultaneously.

- *Sector rules*. The protocol should also factor in rules specific to certain sectors such as those under PECR for telecommunications providers, incoming requirements under the Network and Information Security Directive for digital service providers or operators of essential services and the FCA Handbook for FCA-regulated companies.

- *Other data privacy breach regimes*. Relevant breach notification requirements under non-EU regimes will also need to be factored in to the breach protocol.

An annual mock response to a breach

Whilst such an exercise is time and resource-consuming, it will allow the business to remind itself of, and identify faults or areas for improvement in, its breach protocol. From speaking to companies who have already done this, there are always useful learnings that arise from such exercises.

Timeframe for notification from data processors

The GDPR requires data processors to notify data controllers of data breaches without undue delay. However, many data controllers go further than this and specify a set timeframe - at our Data Protection and Privacy Forum 50% of attendees were planning on requiring processors to notify them within 24 hours of becoming aware of any personal data breach to ensure they could themselves meet the 72 hour deadline for DPA notification.

Third party services available on-demand

The swiftest and most effective responses to security breaches are often provided by, or with the help of, seasoned third party professionals. It would therefore be prudent to engage and

retain on an on-demand basis, for example, data forensics experts who can identify and plug any holes left by any hack and a call centre to deal with questions from individuals. There is unlikely to be sufficient time to choose, approach and contract with such third parties after or at the time of a breach.

Template documents

Consider producing template notifications to individuals, staff, external comms and any regulatory announcements. Likewise template call centre scripts could be produced in advance. Whilst they will need to be customised at the time, having a template to start from which all interested parties have signed off on in advance can save precious time.

Notification form

Finally, it is important for the relevant member of the team to be familiar with the DPA's notification form and the process for submitting it as this can otherwise cause unnecessary delay.

If you have any queries on this Briefing or if you would like to discuss any aspect of the GDPR or any data protection or privacy issue, please do not hesitate to contact Rob Sumroy, Richard Jeens, Richard de Carle, Rebecca Cousin or your usual Slaughter and May advisor.

Rebecca Cousin
T +44 (0)20 7090 3049
E **rebecca.cousin@slaughterandmay.com**

Oliver Howley
T +44 (0)20 7090 3495
E oliver.howley@slaughterandmay.com

Hui Ying Chee
T +44 (0)20 7090 5373
E **huiying.chee@slaughterandmay.com**

Cindy Knott
T +44 (0)20 7090 5168
E cindy.knott@slaughterandmay.com