THE
NATIONAL LAW REVIEW

Impact of EU General Data Protection Regulation on Responses to Data Breaches Involving EU Personal Data

McDermott Will & Emery

Article By
Michael G. Morgan
Romain Perray
McDermott Will & Emery
On the Subject

- Communications, Media & Internet
- Global

- European Union

Tuesday, July 18, 2017

Summary

The forthcoming General Data Protection Regulation will expand the legal obligations of companies that process EU personal data when they suffer a data breach. Every company faces the risk of a data breach that might trigger such obligations so it is critical to prepare for them in advance.

In Depth

The 27 June attack on corporate computer systems around the world is the latest reminder to companies of the need to comply with their obligations under data privacy regulations following a data security incident.

A number of issues arise under existing national and EU data protection laws and the General Data Protection Regulations (GDPR), which comes into force on 25 May 2018. GDPR preparation is an area of intense interest to European companies and companies around the world that process personal data for EU data subjects, many of which will become subject to data protection requirements for the first time under

the GDPR.

The stakes for compliance are high because a failure to comply with the GDPR's data breach notification rules can result in huge fines of up to €10 million or 2 per cent of a company's worldwide annual turnover for the preceding financial year, whichever is higher. Additionally, although laws on data protection class actions in each Member State have not yet been passed, individual data subjects will ultimately be entitled to receive damages in some cases.

Increased Geographical Scope

The GDPR will apply not only to the operations of European companies, but also to companies that do business in Europe or hold European personal data in any way, regardless of whether or not they have subsidiaries in Europe.

This means that companies around the world that process EU personal data will need to prepare for compliance with the GDPR. The most significant requirements include those relating to the transfer of data from an EU Member State to outside the European Union, how personal data is updated and for how long it is stored, and how consent can be given by individuals to companies for the processing of personal data. Additionally, and as discussed below, there are onerous new requirements in relation to data breaches.

Notification Obligations

Currently, amended EU Directive 2002/58 dated 12 July 2002 and EU Regulation 611/2013 dated 24 June 2011 set the standards in the EU for notification requirements after a data breach. Telecommunications service providers are required to notify the relevant national data protection authorities of a "data breach". This obligation could be extended to require companies to notify individual customers whose data has been compromised. Under these EU provisions, no companies outside the telecom sector are required to notify the authorities, although certain pieces of domestic legislation, such as in Ireland or Denmark, require it regardless of the sector involved.

Even for telecoms companies, notification is only required when a data breach occurs in relation to their supply of electronic communication services, thus they are freed from the notification obligation if the breach occurs, for instance, within a company's human resources system. With the GDPR entering into force on 25 May 2018, the days of notification requirements applying only to the telecoms sector will soon be over. The GDPR requires all companies subject to its provisions to notify the competent national authorities within 72 hours of any breaches of personal data if the breach could harm the rights and liberties of the individuals concerned. This type of harm to rights and liberties generally applies to personal data, so it is likely that the notification requirement will apply to most data breaches. In assessing the harm to the rights and liberties of data subjects, it will be necessary to consider:

> "Physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised

> reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."[1]

National authorities will be assessing compliance and, from 25 May 2018, companies will be obliged to keep a record of their data processing, including a general description of security measures. One of the major changes under the GDPR is that data processors will be directly liable, notably if they fail to alert the data controller of a data breach, preventing the controller from fulfilling its notification obligations.

The notification obligations, as expanded under the GDPR, require companies to share almost exactly the same information as was previously required under EU Directive 2002/58 and EU Regulation 611/2013. Companies must therefore ensure they are able to collect the relevant information immediately following an attack.

The information they will need to provide will include the approximate number of data records that were compromised, the number of records and individuals impacted, the probable consequences of the breach, how the company intends to minimize the impact of the breach, and contact details – which is obviously new – for those able to provide additional information, such as the Data Protection Officer.

The obligation to notify individuals whose data is implicated in the breach continues to be based on whether or not the breach represents a "high risk" to them, *i.e.,* to their rights and freedoms, and whether or not the compromised data is illegible to third parties or not. There is, however, the additional burden that data subjects be *individually* notified, in understandable language, unless this is demonstrated to be impossible or disproportionate, in which case a public notification could be made instead.

These obligations, especially the 72-hour notification deadline, pose a considerable compliance challenge for companies. In many data breaches, it is difficult and time consuming to determine whether or not particular records have been compromised.

Delays and difficulties in trying to determine the extent of an attack can occur for many reasons, including insufficient logging of the affected systems, attacker activity, *e.g.,* effective malware and anti-forensic efforts by the attacker, or the compromise of critical log or file data, *e.g.,* the successful encryption by the attacker of the data that is needed to assess individual notification obligations. The most recent wave of malware, known as Petya amongst other names, targets the master boot records of infected computers, thus making the infected machines unusable and complicating attempts to analyse the compromised system. In many breaches, it can take many weeks or months before affected individuals are identified or it is finally determined that those individuals cannot be identified with any degree of confidence.

As a data breach includes the destruction, loss, exfiltration or tampering with a company's data, notification obligations can arise not just from headline-grabbing cyberattacks, but also from system misconfigurations, inadvertent or intentional employee compromises, or other internal errors.

Companies should consider taking steps now to prepare for the possibility of having to notify data subjects on very short notice. These steps could include revising security policies to reflect the urgency of assessing notification obligations, training technical personnel to ensure prompt escalation of security incidents, and preparing a plan for responding promptly to incidents.

---

[1] EU Regulation 2016/679 (GDPR), Recital 85