GDPR and Data Breach News: Are You Ready?

March 5, 2019

News reports of data security breaches with their center of gravity in the European Union continue at a steady pace. Nine months after the EU General Data Protection Regulation ("GDPR") took effect, it is timely to share the latest on best practices for breach preparation and response. Here is a high-level refresher.

Who is a target? Major organizations across economic sectors are among hackers' recent targets in the EU. For example, on January 29, 2019, the French-based IT consulting company Altran Technologies reported it had been the target of a cyberattack affecting operations in several European countries. The company explained the malware was a "crypto locker virus" that was non-detectable by best-in-class firewall and IT defense mechanisms. The following day, Airbus SE reported it had detected a cyber incident on its information systems which resulted in unauthorized access to personal data.

Debevoise & Plimpton

These are just a few examples. National data protection authorities ("DPAs") across the EU have yet to publish definitive data. But all indications are that the DPAs have been swamped—both by breach reports from companies, as well as complaints from affected individuals ("data subjects"). Rough estimates are that companies collectively have reported about 10,000 breaches a month to the DPAs. France's DPA, the *Commission Nationale Informatique et Libertés* (the "CNIL"), reports receiving over 40 complaints per day from data subjects.

The high incidence of breach disclosures is a sharp reminder of the legal challenges and risks associated with data breaches. If the GDPR applies—which may be the case even if the business of a data controller or processor is not based in the EU—then not only does the GDPR mandate that "appropriate" cybersecurity measures be followed in the day to day, but a robust GDPR-compliant incident response plan ("IRP") should be in place, including plans for how to promptly notify the relevant DPAs and data subjects of personal data breaches. If such policies and procedures are not yet in place, it's never too late.

Know what must be notified to the DPAs. GDPR notification obligations do not apply to every security incident, but only to a "personal data breach"—for instance, if there is

an external hack, or an internal accident, resulting in disclosure of personal data. Useful examples of what may constitute a personal data breach are provided in the Article 29 Working Party Guidelines on Personal Data Breach Notification.[1] Nevertheless, uncertainty remains as to when the DPAs expect to be notified. Some DPAs, including the U.K. Information Commissioner's Office, have commented publicly on what they deem to be over-reporting of incidents in the wake of the GDPR.

Get ready to do it promptly. A breach should be notified to the DPA without undue delay, and where feasible, no later than 72 hours after the data controller becomes "aware" of it. What constitutes awareness of a personal data breach will depend on the circumstances of the breach. The goal is to get ready to react promptly. "Tabletops," or personal data breach simulation exercises, may help in that regard. The 72-hour timeframe imposed by GDPR puts a thumb on the scales in favor of early reporting while the company's internal investigation is still in process. As a practical matter, there will rarely be certainty on the facts within 72 hours of first indications of a possible breach.

Identify the relevant DPA. Notification of a breach is usually made to the DPA of the jurisdiction where the breach occurred. However, when a breach takes place in the context of cross-border processing, notification should be made to the "lead" DPA; that is, the DPA in the jurisdiction of the company's main EU establishment. Companies should thus identify their lead DPA in advance. Some lead DPAs may also ask companies to notify DPAs in other EU member states.

GDPR provides that if a company does not have an EU establishment, but regularly offers goods or services to individuals in the EU, then the company should designate a representative in the EU. If a breach occurs, the Article 29 Working Party has recommended that companies notify the DPA in the jurisdiction of that representative. For non-EU established companies that have not yet appointed a representative, it may be prudent to notify the DPA in the jurisdiction with the largest number of potentially impacted individuals, indicating what other jurisdictions might be affected when doing so.

Know the DPA notification channels. The hectic time of a breach response is not the best time to learn the mechanics of DPA notification; rather, best practice is to build these mechanics into the IRP. Many DPA websites now provide online notification forms which allow for breach reports to be submitted through the website or via email

[1] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Pre-GDPR guidance from the Working Party remains valid, now under the auspices of the Working Party's successor, the European Data Protection Board.

(*see, e.g.* online notification forms of the French[2], U.K.[3] and German[4] DPAs). Typically, companies are asked to provide information regarding:

- the nature of the personal data breach;
- the categories and approximate number of affected individuals;
- the approximate number of personal data records affected;
- the name and contact information of the person from whom additional information can be obtained;
- the likely consequences of the breach; and
- the measures taken to address the breach and to limit its potential impact.

For smaller breaches, formal investigations can likely be avoided through detailed disclosures of the breach and the steps that have been (or are being) taken to remediate the cause of the breach.

Be ready to notify data subjects too, where required. Notification to data subjects is required when the breach is likely to result in a high risk to the rights and freedoms of the individuals concerned and should be made without undue delay. The main objective of data subject notification is to provide the affected individuals with information about the steps they should take to protect themselves. Typically, it should include much of the same information that is reported to DPAs as described above. DPAs commonly view prompt notification to potentially affected individuals as a mitigating factor in considering whether to pursue an enforcement action and in setting penalties.

Industry-specific requirements. In addition to the GDPR, several other EU legal instruments[5] impose notification requirements on certain businesses, including providers of electronic communications networks and services. Companies subject to these sector-specific requirements should build these, too, into their IRPs.

Enforcement landscape. In addition to reputational damage and potential legal claims, companies that fail to comply with data protection rules face heavy regulatory fines. At the high end of the penalty range under the GDPR, non-compliance with personal data

---

2 https://notifications.cnil.fr/notifications/index.

3 https://ico.org.uk/media/2614197/personal-data-breach-report-form-web-20190124.doc.

4 *See*, for example, online notification forms of the Hesse Supervisory Authority: https://datenschutz.hessen.de/service/meldungen-von-verletzungen-des-schutzes-personenbezogener-daten or of the Bavarian Supervisory Authority: https://www.lda.bayern.de/en/data_breach.html.

5 *See* Directive 2009/136/EC, Regulation 611/2013, Regulation (EU) 910/2014 and Directive (EU) 2016/1148.

breach obligations may expose companies to fines of up to €10 million or up to 2 percent of their worldwide annual turnover. The following three examples provide a picture of the enforcement landscape.

- In October 2018, the Portuguese DPA imposed a €400,000 fine on a Portuguese hospital for three GDPR violations, including €100,000 for its failure to ensure confidentiality, integrity, availability, and resilience of treatment systems and services. The gist of the concern in this as-yet-unpublished decision was that too many hospital personnel had access to the data of patients for whom the personnel had no treatment responsibility. This fine, believed to be the first-ever data security fine under the GDPR, demonstrated that businesses can be penalized not just for data breaches themselves but for the poor design of their data systems—in this case, overly liberal access controls.

- In November 2018, the Dutch DPA imposed a €600,000 fine on two Uber entities, including the U.S. parent company, for failing to report a personal data breach within 72 hours. Although that ruling was based on a Dutch law predating the GDPR, it illustrates that DPAs will take breach notification delays seriously.

- In January 2019, the CNIL imposed a €50 million fine against Google LLC, which served as a wake-up call for those who still had doubts about the CNIL's determination to enforce the GDPR.[6] In February, the newly appointed head of the CNIL, appearing before the French Parliament, reinforced the message that the CNIL would not hesitate to impose sanctions to assert its authority and credibility.

It is important for companies to keep in mind that, when investigating a data breach, the DPA's review may extend past the breach to include compliance with other GDPR requirements, including the responsiveness of Subject Access Request procedures and processor documentation under Article 30 of the GDPR. Companies thus should be diligent in ensuring that all GDPR requirements are met.

Finally, it is critical to understand that compliance with the GDPR does not equal security. Companies would therefore be well advised to implement robust cyber security measures tied to a cross-functional and well-tested response plan and team, going beyond GDPR compliance, aiming at reducing their exposure to cyber attacks.

* * *

[6] *See* "GDPR Means Business: Google Hit with €50 Million Fine", Debevoise Debrief dated January 28, 2019 available at https://www.debevoise.com/insights/publications/2019/01/gdpr-means-business-google-hit.

With members of its Cybersecurity & Data Privacy group on both sides of the Atlantic, Debevoise is well-placed to assist EU and non-EU businesses on all areas of GDPR compliance, including incident response and interaction with DPAs.

Please do not hesitate to contact us with any questions.

U.S.

Luke Dembosky
ldembosky@debevoise.com

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

PARIS

Antoine F. Kirry
akirry@debevoise.com

Alexandre Bisch
abisch@debevoise.com

Fanny Gauthier
fgauthier@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com

Ceri Chave
cchave@debevoise.com

Robert Maddox
rmaddox@debevoise.com

FRANKFURT

Christopher Garrett
cgarrett@debevoise.com

Dr. Thomas Schürrle
tschuerrle@debevoise.com

Dr. Friedrich Popp
fpopp@debevoise.com