D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

JUNE 2019

DIGITAL MEDIA, TECHNOLOGY & PRIVACY

>> ALERT

GDPR'S INAUGURAL YEAR: MISTAKES MADE AND LESSONS LEARNED

The European Union's (EU) General Data Protection Regulation (GDPR) celebrated its one year anniversary a few weeks ago.

In its first year, data protection authorities (DPAs) in EU member states brought forth over 200,000 cases and dished out over €56,000,000 (equal to over $62 million) in fines; although nearly 90-percent of that amount was imposed on Google alone! Studies show that over 89,000 breach notifications were made, more than 144,000 data subject complaints issued and in excess of 440 cross-border data processing cases initiated in the past year.

The most notable characteristic of GDPR enforcement actions isn't necessarily the monetary value of fines levied; rather, it is the diversity of enforcement activity. Some cases involve more conspicuous violations, such as failure to encrypt and failure to disclose data collection practices; while others involve less obvious violations, such as insufficient security programs and data-subject rights protocols, as well as inadequate consent mechanisms.

THE BOTTOM LINE

In GDPR's inaugural year, except in the case of Google, the low fines indicate that there has been a degree of tolerance for noncompliance as companies continue to determine how to become compliant. However, the past year has shown that no one is immune from regulatory scrutiny, regardless of size, location or industry. It remains to be seen whether regulators will be as forgiving of GDPR violations in year two as they were in year one.

NOTABLE ENFORCEMENTS AND TAKEAWAYS

Google

The largest GDPR fine to date was the €50,000,000 ($57 million) penalty imposed on Google Inc. (Google) by the French DPA Commission Nationale de l'Informatique et des Libertés (CNIL). The CNIL ruled in January that Google violated the GDPR by failing to meet transparency and consent requirements, and failing to clearly disclose their legal basis for processing.

The investigation into Google was sparked by complaints from nonprofit advocacy groups. In a statement, the CNIL said that Google's users were unable to understand the extent of the company's "massive and intrusive" data processing based on the information Google discloses to their users, noting that "the purposes of processing are described in a too generic and vague manner, and so are the categories of data processed for these various purposes." Further the CNIL concluded that the information Google provides to users "is not easily accessible." The violations were classified as continuous violations of the GPDR, rather than one-time violations.

The GDPR gives DPAs discretion to fine up to the greater of €20,000,000 or 4-percent of the company's worldwide turnover. Thus, the Google fine shows that regulators wanted to send a clear message.

Companies should be aware that DPAs may require a business to cease data processing activities altogether, which may be significantly more detrimental than the imposition of mere fines.

>> continues on next page

Knuddels.de

Knuddels.de (Knuddels), a chat app, suffered an intrusion which resulted in the unauthorized disclosure of user personal data. Upon discovery of the data breach, the company reported the incident promptly to the German DPA (LfDI) and notified affected users in accordance with the GDPR's breach notification requirements. During the ensuing investigation, it was discovered that Knuddels stored user passwords in an unencrypted plaintext format, violating security requirements under the GDPR.

The LfDI fined Knuddels €20,000 citing "exemplary cooperation," prompt notification of the security breach, and a significant investment by Knuddels in the aftermath of the breach to update its security measures, which totaled in the six-figure range. The head of LfDi stated, "as a DPA, it is not important for the LfDI to compete for the highest possible fines. What counts in the end is the improvement of data protection and data security for the users concerned."

LfDI's response signals that prompt cooperation and remediation measures, demonstrating a sincere effort to improve, may factor significantly in an investigation and action by a regulator.

Barreiro Montijo Hospital

One of the earliest GDPR fines was assessed by the Portugal DPA Comissão Nacional de Protecção de Dados (CNPD) on Barreiro Montijo Hospital (Hospital). The Hospital was fined €400,000 for violations of basic GDPR principles: data minimization, integrity and confidentiality and implementation of adequate and sufficient technical measures to ensure continued confidentiality and security.

The Hospital was found to allow indiscriminate access to an excessive number of users to its patient management system as a result of inadequate technical and organizational security measures. Among other discoveries, CNPD's audit of the Hospital discovered 985 hospital employees had access rights to sensitive patient health data when there were only 296 physicians at the hospital.

When implementing information security programs, companies must ensure that the six data processing principles of the GDPR are addressed:

1) Lawfulness, fairness and transparency;
2) Purpose limitation;
3) Data minimization;
4) Accuracy;
5) Storage limitation; and
6) Integrity and confidentiality.

Sergic

The French DPA struck again! The CNIL fined real estate company, Sergic SAS (Sergic), €400,000 for failure to implement appropriate security measures. In particular, Sergic's security defect allowed unauthorized third parties to access personal data of rental candidates. Further, Sergic delayed in remedying the defect, only starting remedial efforts six months after becoming aware of it.

In addition to the security failures, Sergic also failed to define and implement data retention periods for certain categories of data that Sergic did not need to retain for extended periods of time. The CNIL noted that the fine was reduced from €900,000 but the final fine remained relatively high for this type of organization.

The importance of adequate security and record retention practices cannot be understated. Even though the GDPR doesn't outline specific security measures, businesses are required to implement technical and organizational measures that ensure security appropriate to the risks involved in processing their personal data.

FOR MORE INFORMATION

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

Oriyan Gitig
Counsel
212.468.4880
ogitig@dglaw.com

Vivian W. Byrwa
Associate
212.468.4927
vbyrwa@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com