View this email in your browser

PRIVACY ENFORCEMENT ACTIONS IN THE EU, THE US AND ISRAEL

11/02/2020

Dear Client,

So much has happened in the privacy world in 2019! It has been a very active year in terms of enforcement actions and we, privacy lawyers, now have a better idea of the direction that the privacy regulators are taking. For this reason, we have put together a brief summary of some of the enforcement actions and fines in the European Union, the United States and Israel involving companies that breached or were alleged to breach their data protection and privacy obligations.

You should read this:

- If your company accesses, has or uses personal data or personally identifiable information (PII);
- If you are an investor or potential acquirer of a company that accesses, has or uses personal data or PII;
- If your company wants to hire a service provider who will access your personal data or PII; or
- If, like us, you simply love privacy and technology!

Amount	Main grounds for the fine	Country
£183 million (intention to fine)	**Insufficient security measures. Data breach**: British Airways suffered a data breach in which website users' data was exposed.	UK
£99 million (intention to	**Insufficient due diligence. Non-detection of data breach**: a well-known hotel group acquired another hotel	UK

fine)	group which had unknowingly previously suffered a data breach in which personal data was exposed. The acquiring group failed to perform sufficient due diligence and remediate the data breach.	
€14.5 million	**Violation of *privacy by design* and *storage limitation* principles**: Deutsche Wohnen SE, a real estate company, violated the "*Data Protection by Design*" and "*Data Protection by Default*" principles by designing an archiving system which recorded personal data of tenants but did not provide a way for the data to be erased after it was no longer necessary.	Germany
€5,000	**Lack of data processing agreement**: Kolibri Image failed to execute a data processing agreement with a service provider. Please reach out to us to discuss the details of this fine.	Germany
€10,000	**Data Protection Officer**: Rapidata GmbH (an internet service provider) failed to appoint a data protection officer.	Germany
€50 million	**Insufficient privacy policy**: A company operating a well-known search engine and other online products did not provide its users with a proper privacy policy that included all the information required under the GDPR, such as categories of data collected, data processing purposes and data storage periods, in a concise, accessible and easy to understand format. **Insufficient consent**: the company did not obtain sufficiently informed consent from its users.	France
€18 million	**Insufficient legal bases**: Austrian postal service processed "special categories of personal data" (i.e. alleged political affinity of affected data subjects) and other data (i.e. package frequency and the frequency of relocations) for the purpose of direct marketing, without the necessary legal bases.	Austria
1.2 million kroner (~ €160,000)	**Insufficient data retention/deletion policies. Violation of the *data minimization* principle**: Danish taxi company Taxa35 maintained a data-retention policy which allowed for personal data to be retained for longer than was necessary. Additionally, the company's attempts regarding anonymization were deemed inadequate.	Denmark
€18,000	**Cookies**: Vueling Airlines's consent-related practices regarding cookies were deemed insufficient (e.g. the consent mechanism was not considered sufficiently granular)	Spain
€15,000	**Cookies**: Jubel.be – a small Belgian company who operates a website with legal information – failed to provide sufficient information regarding the cookies used on the website. Its cookie policy was only available in English (despite the fact that the website targeted French and Dutch-speaking readers). The company did not provide any opt-out mechanism for certain types of cookies and the consent obtained was not deemed sufficiently granular. Furthermore, there was no easy way for users to withdraw consent. **Interesting note**: the Supervisory Authority did not act based on a user complaint but instigated the investigation and proceedings on its own initiative.	Belgium
€70,000	**Unlawful monitoring**: Louis Group used the *Bradford factor* for profiling and monitoring sick leave and employee	Cyprus

	absenteeism in violation of Article 6 and Article 9 of the GDPR.	
€5,000	**Non-compliance with data subject rights**: a request for access to a patient's medical file was not satisfied by a hospital because the dossier could not be identified/located.	Cyprus
$174 million (settlement with FTC)	**Violation of COPPA rules. Children's data**: the FTC and New York Attorney General alleged that a well-known video platform violated the COPPA rules by collecting personal information—in the form of persistent identifiers that are used to track users across the Internet—from viewers of child-directed channels, without first notifying parents and getting their consent.	USA
$575 million (settlement with FTC)	**Insufficient security measures. Data breach**: the FTC alleged that Equifax failed to secure the massive amounts of personal information stored on its network, leading to a breach that exposed millions of names, dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud.	USA
NIS 100,000	**Various violations**: A company did not register its database containing personal data with the Israeli Law, Information and *Technology Authority*. The company also used personal data which was illegally obtained and used some of the data for marketing purposes without meeting the obligations required in order to do so under Israeli privacy regulations.	Israel

As the GDPR matures and additional privacy laws and regulations are passed (such as the California Consumer Privacy Act (CCPA), which became applicable on the first of January), it is likely that we will see a rise in the volume and size of the fines which companies receive due to breach of their data protection and privacy obligations.

The above enforcement actions emphasize the importance of allocating appropriate resources to privacy-compliance programs and underscore the importance of addressing cybersecurity risks as an aspect of good corporate governance. This does not have to be an exhausting exercise and we believe that compliance programs should be adjusted to each company's data processing practices and resources.

Please feel free to contact us if you have any questions about the fines or would like to discuss your company's compliance with applicable data protection and privacy regulations.

Contact Information

Ignacio Gonzalez Royo, Partner
Technology group
+972-3-6103199
ignaciog@meitar.com

Nicole Denise Feld, Associate
Technology group
+972-3-6103100
nicolef@meitar.com

For additional information about our firm's Technology group, click here.
