GDPR Penalties and Type of Violations

Under the General Data Protection Regulation (GDPR), supervisory authorities can fine violators or take other punitive actions. Punitive actions can include:

- issuing warnings and reprimands
- imposing temporary or permanent bans on data processing
- ordering the rectification, restriction, or erasure of data
- suspending third country data transfers

Most companies tend to worry the most about potential fines because the caps are set at extremely high levels.

In the largest fine to date, British Airways was fined €204 million following a website attack that exposed ~500,000 customer records. The attack was tied to poor cybersecurity.

Also in the travel industry, UK Marriott was fined €123 million due to an ongoing central reservation database hack in the Starwood system from 2014-2018 (UK Marriott had acquired Starwood before discovering the hack).*

Google was fined €50 million in France for failure to comply with GDPR obligations. Google's fine stemmed from failure to provide users enough information to users about its data consent policies.

GDPR Penalty Tiers

In determining how to penalize infringing companies under the GDPR, supervisory authorities are tasked with reviewing infractions on a case specific basis and assigning penalties that are "effective, proportionate and dissuasive." The maximum fine for a GDPR violation is 2% of annual global turnover or €10 million (whichever is *greater*) for a tier 1 infringement. And 4% of a company's annual global turnover or €20 million (whichever is *greater*) for a tier 2 infringement.

GDPR Tier 1 Infringements

Tier 1 infringements are GDPR violations that are based on infringements of:

- Article 8 conditions for children's consent
- Article 11 processing that does not require identification
- Articles 25-39 general obligations of processors and controllers
- Article 42 certification
- Article 43 certification bodies

GDPR Tier 2 Infringements

Tier 2 infringements are GDPR violations based on infringements of:

- Article 5 data processing principles
- Article 6 conditions for consent
- Article 9 processing special categories of data
- Articles 12-22 data subjects' rights
- Articles 44-49 data transfers to third countries and/or international organizations

GDPR Fines

Unlike the CCPA privacy regulation out of California, the GDPR does not attempt to target specific types of industries. While the CCPA is geared towards regulating large entities or companies engaged in direct marketing activities and creates carve-outs for nonprofits, the GDPR is geared toward any data collection and processing that occurs in Europe or targets Europeans.

Entities in all sectors and of all sizes that are established in Europe or collect or process the data of people in Europe need to aim for GDPR compliance. In 2019, major GDPR fines hit multiple sectors for violations ranging from illegal sale of information to security breaches to insufficient identity validation.

Improper/Illegal Data Collection

The Spanish soccer league (La Liga) was caught violating the GDPR's transparency provisions. La Liga turned on app users' microphones remotely during soccer matches. They then listened in order to identify locations where they could hear the games being watched. They used the information to sue 600 bars for pirating the game streams.

In addition to the transparency violations, La Liga had also failed to allow its app users to later withdraw their consent. (Sidenote–if you're going to do something illegal, it's a bad idea to use it as your evidence in your lawsuit. La Liga has denied the allegations and plans to appeal the decision.)

Security Breaches

The Marriott and British Airways fines, both arising from security breaches, are the largest we have seen. In fact, security breach violations are considered so serious that even Bulgaria's tax authority, the National Revenue Agency, was fined €2.6 million for a security breach that exposed the records of 6 million people.

Security breaches can also result in additional fines if companies do not report the breach to the appropriate authorities or individuals in a timely fashion. Uber failed to report a security breach within 72 hours, resulting in a €600,000 fine.

Improper Sale

The Austrian Post was fined €18 million for selling detailed personal profiles of approximately 3 million Austrians to political parties and companies.

Off-shoring

The GDPR is also serious about the storage of data in non-GDPR regulated countries.

Futura Internationale, a French energy company with fewer than 100 employees, was fined €500,000 for GDPR violations. The company did marketing via call centers outside of the EU, so the fine included failure to provide adequate protections when transferring PI outside of the European Economic Area.

In addition, they failed to limit the processing to what was necessary. Failure to inform data subjects, failure to respect consumers' objections to processing, failure to cooperate with the supervisory authority. While this fine is significantly smaller than some of the others listed, it is still significant, and it was levied against a smaller company.

Storage

In Germany, Deutsche Wohnen, a leading European real estate agency, was fined €14.5 million for unlawfully storing current and former tenant information in an archive system that did not include the ability to delete old data.

Security

Companies have also been fined for not having sufficient protections against the sharing of customer data.

The German company 1&1 Telecom was fined €9.5 million because personal information was available for anyone who gave them the name and date of birth of a customer.

UWV, a Dutch insurance service provider, was fined €900,000 for its failure to put multifactor identity protections on its employer portal.

The Oslo Municipal Education Department was fined €200,000 for exposing student information in a mobile app that had not been designed or tested for privacy and security standards.

Data Scraping

For companies that rely on publicly available data, it is important to remember that the GDPR does not give you a free pass on collecting and processing the data.

The Polish Supervisory Authority fined a company €220,000 for scraping data from public registries to create trade reports and contact lists it shared with its clients. The company had collected approximately 7.6 million records and made some attempt to comply with the GDPR notice of processing requirements. It sent an email to all of the individuals for whom it had an email address (~680,000), but it did not provide any notice to the ~6.5 million other individuals.

The company made multiple mitigating arguments, including that it was using publicly available information, limited the data (contact details only), and had high levels of security. Its most important argument for our purposes was that the cost of sending mailed notice would have been over €7.8 million for postage alone. Notice by anything other than email would, in their view, require a “disproportionate effort” under the GDPR and so could be avoided.

The Polish Authority disagreed and found that the company had intentionally violated the GDPR. (If you’re doing the math and thinking the fine was worth it, the supervisory authority also ordered the company to follow through and send notice to all the individuals involved).

GDPR Penalties In Summary

While it is still too early to make predictions regarding GDPR fines, it is clear that all sectors of the economy, from government to private industry, from education to travel, need to evaluate their GDPR responsibilities and take action.

As shown by the Polish example above, even companies that have taken some steps toward compliance are not safe from regulatory action.