HBR
CONSULTING

# GDPR: Are the Fines Real?

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400

## Introduction

Under the General Data Protection Regulations (GDPR), organizations may be fined up to €20 million, or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[1] In January 2019, the French Data Protection Authority fined Google €50 million for GDPR violations. When the European Union's GDPR went into effect in May 2018, many organizations feared heavy fines based on GDPR violations.[2] Big headlines such as the fine issued against Google reinforced this perception. While the potential for large fines is real, organizations may find it helpful to understand the context of the current fines issued based on GDPR violations, and how that may or may or may not relate to them.

## Who Are Filing the Complaints?

Most actions are initiated by complaints filed with data protection authorities, not random data protection inspections by government agencies. Two of the leading data protection advocacy organizations are None of Your Business (NOYB) and La Quadrature Du Net. These are the organizations that filed the initial complaint that resulted in the Google fine. Almost immediately after the GDPR went into effect, NOYB and La Quadrature Du Net filed complaints against Apple, Facebook, Google, Instagram, LinkedIn and WhatsApp.[3] Currently, NOYB is targeting streaming companies like Netflix, Spotify and YouTube.[4]

Other sources of complaints are data subject access requests (DSARs). Under the GDPR, people ("subjects") can contact organizations and require the organization to confirm they retain personal data on that subject and provide a copy of the personal data they retain.[5] Organizations have 30 days to respond to these requests. When an organization fails to respond, the subject can file a complaint with their national protection authority. Enough of these complaints will trigger an investigation.

Most actions are initiated by complaints filed with data protection authorities, not random data protection inspections by government agencies.

## What are the Bases for Current GDPR Actions?

The enforcement of the GDPR is the responsibility of national protection authorities within the European Union.[6] Each E.U. member state is responsible for establishing a supervisory authority to monitor the application of the GDPR and protect the "fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union."[7] Similar to the enforcement and application of the prior European Data Protection Directive, some countries participate more actively in the protection of personal data. For this analysis, we will examine the following four active jurisdictions' enforcement of the GDPR: the United Kingdom, France, Germany and The Netherlands.

## United Kingdom Information Commission Office (ICO)

Since the implementation of the GDPR, the ICO has issued over 25 fines for data protection violations. Some of these violations were based on the previous law/directive. The fines range from £4,350 for failure to pay the ICO data protection fee to £385,000 and £500,000 against Uber and Equifax, respectively, for failing to protect customers' personal information during a cyberattack, to £500,000 against Facebook for "serious breaches of data protection law." Excluding the administrative fines for failing to pay the data protection fee, fines average around £155,000.

Most of the ICO's actions are based on the following violations: (1) sending large amounts of unsolicited emails, text messages, phone calls or direct marketing materials without the required consent; (2) cyberattacks and failure to secure personal information; and (3) data brokers collecting and selling personal information for political marketing purposes.[8]

## France National Commission on Information and Liberty (CNIL)

The CNIL is the agency that issued the €50 million fine against Google. Since the implementation of the GDPR, the CNIL has issued nine financial sanctions. Most of the CNIL sanctions focus on cyberattacks and failure to secure personal data.[9] These fines range from €30,000 to €400,000, with an average fine of approximately €176,000 for violations based on failure to secure personal data. The CNIL also fined an employer €10,000 for having a fingerprinting system (i.e., biometrics) for controlling employee hours without obtaining proper consent from its employees. It is important to note that in this case the employer received serval warnings before the CNIL issued the fine.[10]

## Germany Federal Commission for Data Protection and Freedom of Information (BfDI)

The BfDI will not be releasing official activity reports for 2017 and 2018 until May 2019.[11] The first known sanction by the BfDI was a €20,000 fine in November 2018 against a social media company for failing to secure personal data. Some raised concerns about the low fine, but it should be noted that the low fine was the result of the company's immediate notification to the BfDI of the security breach.[12]

## Netherlands Autoriteit Persoonsgegevens (AP)

In 2018, the AP put an emphasis on data breaches or "data leaks." These were especially evident in the healthcare, financial services and public government sectors. Of the 20,000+ data breaches reported to the AP, the AP investigated 298 cases. Most investigations resulted in a warning. The AP did fine Uber €600,000 for a data leak, but the higher fine was a direct result of Uber's failure to promptly notify the AP and those impacted.[13]

## What Can We Learn from the Current Enforcement?

- **Emphasis on consumer data.** Enforcement of the GDPR is primarily focused on the personal data of consumers. Consumers may be defined as potential buyers of goods and services, healthcare patients and potential voters. The focus on consumer data is evidenced by the frequency of fines issued for direct marketing (unsolicited phone calls, mailers, emails and texts). Based on the current enforcement, we are not seeing any business-to-business enforcement or efforts to find personal data that is not used for marketing in the metadata of organizational systems. Additionally, we are seeing very little enforcement associated with employment data.
- **Personal data security breaches.** Some of the largest fines are the result of cyberattacks where it was determined (1) there were insufficient controls to protect the data, and (2) the organization failed to notify the relevant national protection authority and those impacted by the personal data breaches.
- **Failure to respond.** Organizations must be prepared to respond to both consumers who file DSARs, and national protection authorities requesting information or changes in organizational policies associated with personal data. In most cases, national protection authorities will issue a warning for minor violations so long as the organization properly responds to the requests.
- **Warnings for minor violations.** National protection authorities are not imposing large fines for minor GDPR violations. Most large fines are based on major unsolicited marketing campaigns, data breaches combined with a failure to notify, and large organizations that were the initial target of the law (e.g., Google and Facebook). According to the UK's ICO Commissioner Elizabeth Denham, "when we do need to apply a sanction, fines will not always be the most appropriate or effective choice. … Compulsory data protection audits, warnings, reprimands, enforcement notices and stop processing orders are often more appropriate tools. … Hefty fines can and will be levied on those organisations that persistently, deliberately or negligently flout the law."[14]

Some of the largest fines are the result of cyberattacks where it was determined there were insufficient controls to protect the data, and the organization failed to notify the national protection authority and those impacted by the personal data breaches.

## Conclusion

Evidence shows that fines under the GDPR are real, but they are also predictable and not typically imposed for minor violations. Organizations wishing to mitigate the risk of paying fines associated with GDPR violations can take the following actions:

1. Identify, minimize and protect personal data retained by the organization.
2. Obtain data subject consents before engaging in a marketing campaign that uses personal data
3. Respond promptly to SDARs and actions from national protection authorities.
4. Provide proper notification in the event of a data breach.

## Connect With Our Experts

**Laurie Fischer**
Managing Director

**O** 312.638.5127
**E** LFischer@hbrconsulting.com

**Tom Corey**
Senior Manager

**O** 312.638.5125
**E** TCorey@hbrconsulting.com

## Sources

[1] Reg. (EU) No 2016/679, Art. 83(5).

[2] CNIL Deliberation No. SAN-2019-001, January 21, 2019. https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1

[3] Meyer, David, "Activists Are Already Targeting Google and Facebook Over Europe's New Data Privacy Law That Went Live Today," *Fortune Magazine,* May 25, 2018. http://fortune.com/2018/05/25/google-facebook-gdpr-forced-consent/

[4] "Netflix, Spotify & YouTube: Eight Strategic Complaints filed on "Right to Access," *NOYB – European Center for Digital Rights*. https://noyb.eu/access_streaming/

[5] Reg. (EU) No 2016/679, Art. 15. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

[6] Reg. (EU) No 2016/679, Art. 51.

[7] Reg. (EU) No 2016/679, Art. 51(1).

[8] "Enforcement action," *Information Commissioner's Office*. https://ico.org.uk/action-weve-taken/enforcement/?facet_type=Monetary+penalties&facet_sector=&facet_date=&date_from=&date_to=

[9] "Sanctions," *Commission Nationale de l'Informatique et des Libertés*. https://www.cnil.fr/en/tag/sanctions

[10] "Biométrie au travail illégale : sanction de 10.000 euros," *Commission Nationale de l'Informatique et des Libertés,* September 20, 2019. https://www.cnil.fr/en/node/24806

[11] "Activity Reports on Data Protection," *BfDI.* https://www.bfdi.bund.de/DE/Infothek/Taetigkeitsberichte/taetigkeitsberichte-node.html

[12] Schmidt, Oliver, "Germany's First Fine Under the GDPR Offers Enforcement Insights," *IIAP,* November, 27, 2018. https://iapp.org/news/a/germanys-first-fine-under-the-gdpr-offers-enforcement-insights/

[13] "Figures Data Leaks 2018," *Autoriteit Persoonsgegevens (AP).* https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/cijfers-datalekken-2018

[14] Macaulay, Tom, "Information Commissioner Elizabeth Denham dispels GDPR myths," *ComputerworldUK,* May 3, 2019. https://www.computerworlduk.com/data/information-commissioner-elizabeth-denham-dispels-gdpr-myths-3676726/

HBR
CONSULTING

HBR Consulting (HBR) delivers advisory, managed services and software solutions that increase productivity and profitability, while mitigating risk for law firms, law departments and corporations. As trusted advisors with deep industry experience, clients partner with HBR to achieve significant, sustainable results.

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400


advisory | managed services | software solutions | insights