Why should business leaders be concerned about GDPR fines?

Since the European Union's General Data Protection Regulation (GDPR) came into force in May 2018, it has had a powerful impact on the international privacy landscape.

A New Era for Data Privacy

- Businesses and other organizations have been forced to design new privacy management programs, draft new privacy policies, appoint data protection officers and reassess their relationship with data privacy.
- Many governments have responded either by introducing new privacy legislation or amending existing laws to modernize their privacy regimes.
- The potentially significant fines that could result from GDPR violations – up to a maximum of €20 million or 4% of the company's annual worldwide turnover for the preceding fiscal year, whichever is greater[1] – have become a top concern for many business leaders.
- Since its inception, European national data protection authorities have imposed some 400 fines amounting to approximately €250 million[2].

Notable GDPR Enforcement Actions

In July 2019, the UK's Information Commissioner's Office (ICO) announced fines of £183 million[3] against British Airways and £99 million[4] against Marriott International Inc. Both fines were the result of data breaches.

In October 2020, the ICO considerably reduced the fines. The British Airways fine was reduced by 89% to £20 million[5]. The Marriott fine was reduced by 81% to £18.4 million[6]. The ICO reportedly considered the adverse impact of the COVID-19 economic lock-down in making this decision.

---

1 **https://gdpr-info.eu/issues/fines-penalties/**

2 GDPR Enforcement Tracker. Retrieved from **https://www.enforcementtracker.com/?insights** [October 2020]

3 **https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/**

4 **https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/**

5 **https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/**

6 **https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/**

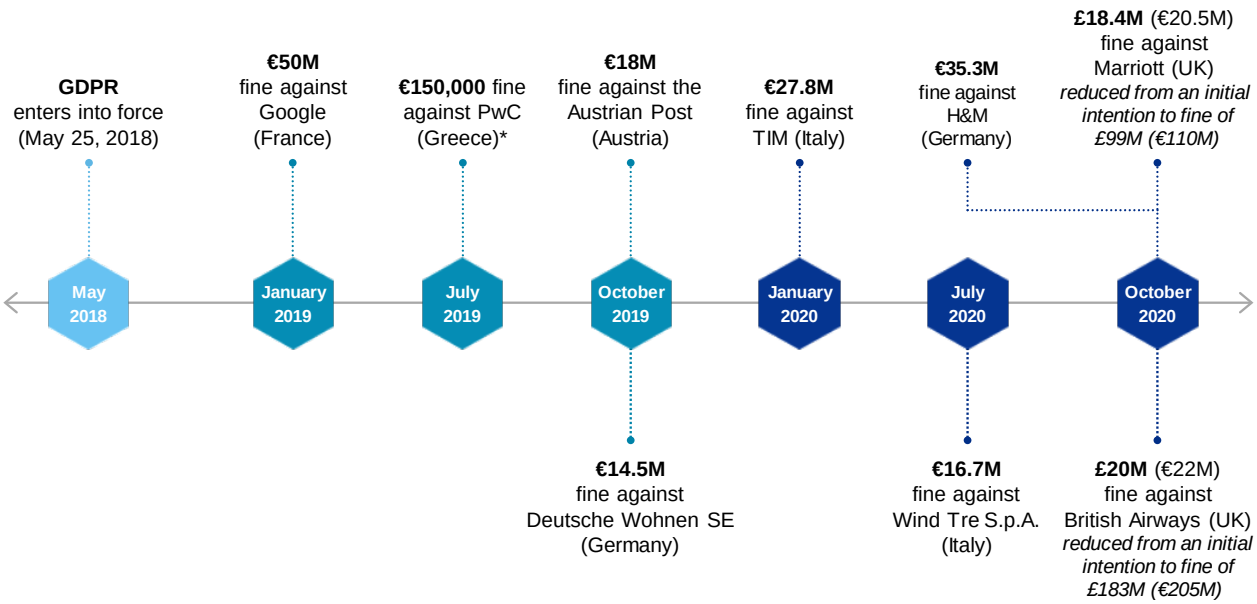
Release Date: November 2020

Following these reductions, the highest monetary penalty to emerge since the GDPR's entry into force is the January 2019 fine against Google imposed by the French data protection authority (CNIL)[7] for a breach of transparency and information duties, as well as failure to obtain valid consent, related to the personalization of ads. The €50 million[8] fine was confirmed on appeal in June 2020.

The Italian data protection authority has issued a total of €46 million in GDPR fines in 2020 alone, the highest of all EU member states during that time[9]. A €27.8 million[10] fine against Italian telecommunications operator TIM was imposed in January 2020 mainly because of unlawful data processing and a non-compliant marketing strategy.

Considerable enforcement action has also been noted in Germany. In October 2020, Hamburg's data protection authority[11] announced a €35.3 million fine[12] against H&M. The Swedish clothing retailer was penalized for the unlawful collection and storage of information pertaining to the personal lives of its employees.

Timeline of Notable Fines until October 2020



* First fine against an accounting firm

7 *Commission nationale de l'informatique et des libertés*

8 **https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc**

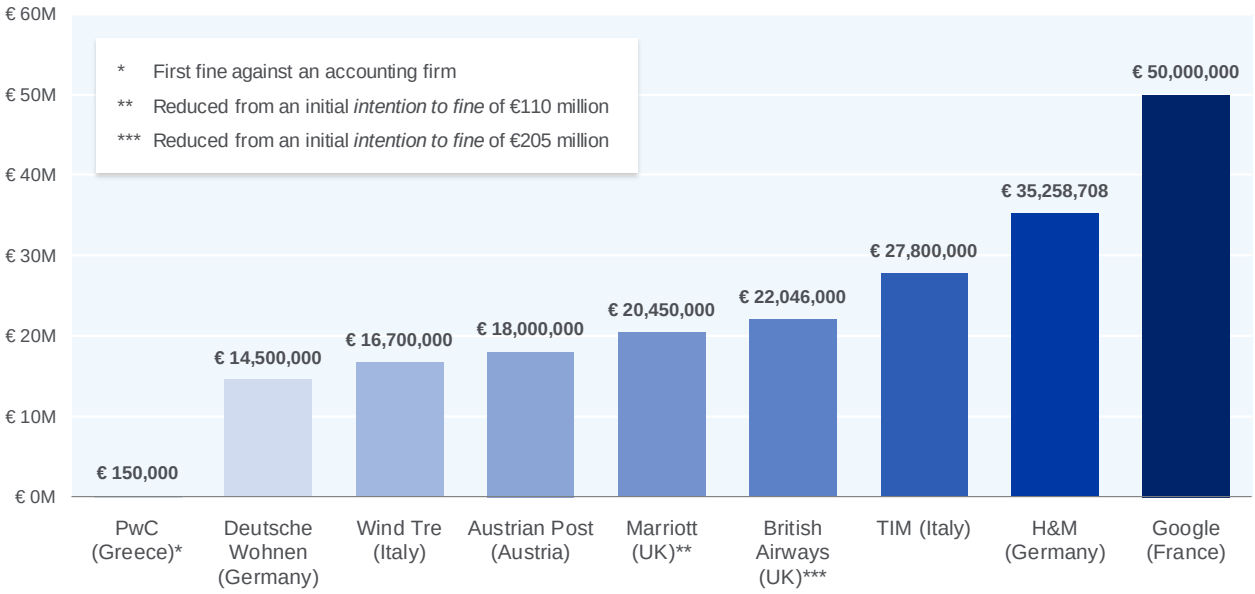
9 **https://dataprotection.news/italy-tops-gdpr-penalty-list-with-e46m-worth-of-fines-this-year/**

10 **https://dataprivacymanager.net/e278-million-gdpr-fine-for-italian-telecom-tim/**

11 *Hamburg Commissioner for Data Protection and Freedom of Information* (HmbBfDI)

12 **https://www.allenovery.com/en-gb/global/news-and-insights/publications/gdpr-fine-for-data-privacy-breach**

Notable GDPR Fines | May 25, 2018 to October 2020



On the Horizon

Despite the reductions in the British Airways and Marriott fines, the potential for large monetary penalties remains a very real risk for business leaders. The average monetary value of the top ten GDPR fines is over €20 million – the nominal threshold for large administrative fines as referred to by article 83 of the GDPR.

Given multiple ongoing investigations – notably including those being undertaken by Ireland's Data Protection Commission – significant enforcement decisions may still be forthcoming. Aon will continue to monitor major developments relating to the enforcement of the GDPR and its overall impact on the data privacy landscape.

Aon Resources

Aon's Cyber Solutions and DLA Piper have published the 3rd Edition of *'The Price of Data Security: A guide to the insurability of GDPR fines across Europe'.*

If you would like to discuss any of the issues raised in this article, please contact **Rona E Davis**.