GDPR fines across the EU and their implications

Stephanie Pritchett and Ben Wootton, Partners, and Hilary Homer, PC.dp. Data Protection Practitioner, with Pritchetts Law LLP, investigate trends in GDPR fines levied in the past year, and consider how organisations can help to future-proof themselves against fines

European Supervisory Authorities have levied more than €160 (£138) million in fines under the GDPR over the last 12 months — nearly triple the figure of €57 (£49) million that was recorded for May 2019 to May 2020. Before we explore the reasons for this apparent surge, it is worth recalling that fines are just one of the tools at regulators' disposal. Supervisory Authorities often use other methods of encouraging compliance, for example, regulatory audits, enforcement action, naming and shaming via undertakings, and so on.

It is not just fines that affect an organisation's bottom line — any enforcement action will often do so. For example, enforcement action might result in the costs of:

- establishing internal and external resources to change systems and processes, or to comply with individual rights requests in progress (for example, enforcement of data deletion where data were unlawfully obtained);
- managing investigations or audits;
- writing to customers, employees and suppliers about an actual or suspected security breach and the loss of business or trust and confidence that may result;
- being exposed to reputational damage; and
- compensating individuals, whether officially through court-imposed compensation or through goodwill gestures to try to avoid more formal action.

Supervisory Authorities can also impose restrictions on the international transfer of personal data. Given the current landscape, it is only a matter of time before this tool is used more routinely. The imposition of such restrictions risks creating huge interruption for organisations along with massive financial aftershocks.

This article reviews the largest fines issued by EU Supervisory Authorities, and comments on what they mean for organisations.

Administrative fines in the GDPR

As a reminder, Article 83 of the GDPR establishes two tiers of administrative fine.

Lower-tier fines: These go up to €10 million (£8.7 million under the UK GDPR), or up to 2% of an organisation's total worldwide annual turnover, whichever is higher. Lower-tier fines are imposed in breaches involving contraventions of the GDPR's requirements on privacy by design and by default, data security and breach notification, data protection impact assessments ('DPIAs'), the role and responsibilities of the Data Protection Officer ('DPO') and certification (Articles 8, 11, 25–39 and 40–43 of the GDPR).

Higher-tier fines: These go up to €20 million (£17.5 million under the UK GDPR), or up to 4% of an organisation's total worldwide annual turnover, again, whichever is higher. Higher-tier fines are imposed for breaches of the core data protection principles, lawfulness of processing and the conditions for consent (Articles 5–7); the fundamental privacy rights of data subjects (Articles 12–22), including their rights to access their data (Article 15), have them corrected (Article 16) and have them erased (Article 17, also known as 'the right to be forgotten'); and the provisions on international data transfers (Articles 44–49).

There are many factors at play when regulators are determining the seriousness of the infringement and therefore the appropriate type of penalty. These include:

- the number of data subjects affected as a proportion of the total pool;
- the purpose of the processing;
- the damage suffered by data subjects;
- how long the infringement lasted; and
- whether the organisation had implemented appropriate technical, organisational and security measures, or implemented a regulator's previous recommendations.

Therefore, as an example, an isolated failure connected to a data subject access request ('DSAR') is unlikely to warrant a higher-tier fine, but where it leads to identification of problems that are endemic within the offending organisation, the regulator could determine that a fine in that tier would be appropriate.

Significant fines levied

H&M (Germany): In the 12 months prior to June 2021, the largest financial penalty to have been imposed was that on retailer H&M by the State Data Protection Commissioner in Hamburg, which issued a fine of over €35 million (£25 million) — the second highest since the GDPR came into force — in October 2020 for H&M's unlawful use of employees' data. The retailer was found to have collected, stored and exposed data on the private lives of its staff, including special category data such as health information and religious beliefs.

British Airways and Marriott International (UK): In the same month, the UK data protection regulator, the Information Commissioner's Office ('ICO') imposed two huge fines. One was on British Airways ('BA'), which the ICO fined over £20 million (€22 million) after a breach whereby the personal and financial details of more than 400,000 of its customers were unprotected. The other was issued to Marriott International ('Marriott') and totalled over £18.2 million (€20 million) for failing to keep secure the personal data of 383 million customers.

TIM (Italy): In January 2020, the Italian regulator, the Garante, issued its largest fine to date. It imposed a €27.8 million (£24 million) fine on TIM, a telecommunications provider, for a series of GDPR violations including data processing relating to the receipt of unwanted promotional calls, which was carried out without the data subjects' consent.

Google (France): Each of the fines above was overshadowed by the largest fine to be imposed since the GDPR came into force. In January 2019, the CNIL ordered Google to pay €50 (£43) million for violating privacy laws. The CNIL launched its investigation into Google's ad personalisation process after receiving complaints from consumer groups. It drew two conclusions that contributed to the enormity of the fine:

- Google violated Article 12 of the GDPR by breaching its obligations to act transparently and provide information in a way that users could easily access. The CNIL found that certain information about the collection and processing of data was only accessible after five actions by users. Even after users had located the information, the content was unclear about what Google was doing with their data; and
- Google violated Article 6 of the GDPR by collecting personal data illegally. It did not have a legal basis for processing users' data to provide personalised advertisements. Google had relied on data subjects providing generalised consent for all of its processing purposes. However, under the GDPR, consent must be specific and provided for each processing purpose.

The CNIL declared Google's processing of personal data to be 'massive and intrusive in nature'.

Fines issued by Supervisory Authorities between May 2019 and May 2020

Supervisory Authority	Number of fines levied	Total value of fines (€)
Germany	6	410,607
Italy	12	39.4 million
France	4	1.1 million
UK	1	320,000

Fines issued by Supervisory Authorities between May 2020 and May 2021

Supervisory Authority	Number of fines levied	Total value of fines (€)
Germany	6	48 million
Italy	58	32.3 million
France	9	3.5 million
UK	3	43.9 million

General trends

Outliers to one side, a general trend can be identified: there has been an increase in the frequency of fines since the GDPR's introduction three years ago. In some ways, this is not a surprise — it takes time to initiate regulatory investigations and bring them to a conclusion. However, with the GDPR now having reached its third anniversary, we can also interpret the increase in the number and size of fines as a sign that regulators are taking an increasingly tough stance on data protection infringements.

Another clear trend is the increase in breach notifications. 2020 saw an increase in breach notifications of nearly 20% on the previous year. However, the number of breach notifications by country doesn't necessarily correlate with the fines that their regulators levy. In fact, Italy and France — the countries that recorded the lowest number of breach notifications — had the highest figures for fines. The tables above compare the fines that were levied by selected European SAs year on year. If we exclude the Italian fine on TIM (an

(Continued on page 10)

(Continued from page 9)

outlier) these figures indicate a massive upswing in the value of fines that have been imposed by these four SAs.

It is worth noting that there have been several successful appeals and massive reductions in fines issued by regulators. For instance, in the UK, the ICO's proposed fine on BA plummeted from over £177 million (€205 million) to around £19 million (€22 million), and its fine on Marriott dropped from £96 million (€111 million) to around £17 million (€20 million). The reductions happened as a result of the ICO taking into account each organisation's attempt to mitigate the effects of the incident, their commitment to improvements and the economic impact of the Covid-19 pandemic. Commentators have suggested, perhaps cynically, that large multinational organisations know that regulators have a much more limited budget to fight fines, and may eventually give up appeals or accept lower fine proposals. The accuracy of these suggestions depends on the support given nationally to those regulators to do their job. Some regulators with smaller budgets and many multinationals to regulate (it's hard not to mention the Irish Data Protection Commission here) may well find this a struggle. Despite this, many of the regulators that have issued fines have robustly defended them.

Lessons learned

So how can organisations future-proof themselves in a landscape of larger and more frequent GDPR fines, albeit with an increased incidence of appeals? Let's return to the five significant fines considered above and analyse where those companies went wrong and what can be done differently.

H&M: There are various legitimate reasons for organisations to conduct interviews with their employees and record their findings, including surveys, appraisals, back-to-work interviews and exit interviews. However, it is essential that organisations fully understand the information that they are processing, why they are processing it and the appropriate legal basis for doing so. They should consider whether it is necessary to conduct or refresh any DPIAs or legitimate interest assessments ('LIAs'). It might also be a good time to conduct an independent audit to check whether staff compliance and governance processes are still fit for purpose. This is particularly relevant in light of the pandemic and the shift towards hybrid working environments.

British Airways: The ICO found that BA had been negligent in maintaining its operating systems, which suffered from significant vulnerabilities and shortcomings. BA didn't detect the attack itself; instead, it was alerted by a third party over two months later. The ICO was uncertain as to whether BA would have detected the attack itself at all, which was a major factor in the scale of the fine that it handed down. Organisations should scrutinise their IT setups and ensure that all appropriate data security measures are implemented — including by the organisation's suppliers — and that their processes for identifying and notifying breaches are up to date and work properly. The organisation would not necessarily need to incur excessive costs in doing so. In the case of BA, several measures were available on its existing systems, but had not been adopted.

Marriott: In contrast to BA's prompt notification of the breach, Marriott only notified the ICO and affected data subjects of its breach two months after becoming fully aware of the nature of it. Managing the breach identification and reporting process, and meeting the GDPR's reporting deadlines, are key to mitigating potential enforcement action. Organisations should examine their systems to ensure that they can recognise a breach and review their breach-reporting procedures. They should also provide training to staff to ensure that they know what internal security measures are in place, can recognise security breaches and can comply with the prompt reporting obligations that are set out in the GDPR. In addition, organisations must ensure that they recognise a data breach as a key strategic risk, and prioritise the provision of appropriate cyber security expertise and oversight from board-level stakeholders.

TIM: Organisations should ensure that their marketing activities are fully compliant with the GDPR and the Privacy and Electronic Communications Regulations. They can do this by, for example, reviewing how marketing service providers are behaving and assessing the transparency of their privacy notices. They should ensure that any consents requested are valid (unambiguous and unbundled), recorded and refreshed. Organisations should test their processes so that when consent to marketing is withdrawn, this is accurately recorded and adhered to.

Google: As with the issues with TIM's apps, Google was fined for a lack of transparency and accessibility around the collection and processing of data, and reliance on bundled consent. The magnitude of the fine levied on Google should in itself inspire organisations to assess their GDPR compliance programmes and ensure that they are fit for purpose. As part of this, organisations must carefully analyse what data they collect about customers and track the legal basis under which they do so. A good way to do this is by creating and regularly maintaining a record of processing activity.

In summary then, organisations should review their data protection processes, policies, training and security practices carefully, ensuring that they really are GDPR-compliant, and documenting and risk-assessing their data-processing activities appropriately. If organisations have been subject to fines or other enforcement action, they must be diligent about putting new practices in place to avoid infringements being repeated in future. SAs are likely to check that their recommendations have been implemented in line with Article 83 of the GDPR, and can increase fines where this is not the case.

Stephanie Pritchett, Ben Wootton and Hilary Homer
Pritchetts Law LLP
hilary.homer@pritchettslaw.com
stephanie@pritchettslaw.com
ben.wootton@pritchettslaw.com