Global data risk

The most active regulators, the biggest fines – and the conduct in the spotlight

Freshfields Bruckhaus Deringer

The most active regulators, the biggest fines – and the conduct in the spotlight

Personal data has become a critical source of value – and regulatory risk – for businesses. The threat is particularly stark in Europe where the advent of the General Data Protection Regulation (GDPR) has altered the landscape dramatically. In this report, we examine the evolution of GDPR enforcement, identifying the most active EU authorities and those that levy the biggest fines. We take a deeper dive into the decisions themselves to reveal how agencies treat different types of misconduct and how they calculate penalties. And we look at fines issued under the GDPR alongside penalties handed out by the world's hardest-hitting authorities to build a global picture of data enforcement.

Introduction and methodology

- This study looks at all penalties levied by EU data protection authorities (DPAs) under the GDPR from its inception to February 2021. We have set this enforcement activity in context by compiling a list of the 100 biggest data fines issued across Europe and North America – where the world's harshest sanctions originate – between 2017 (the year before the GDPR came into force) and February 2021. In Europe, our analysis includes penalties issued under member states' national data protection and e-commerce laws.

  In addition, we have overlaid insights on the emerging threat of data-related litigation and explored wider regulatory trends across the world, including Brexit and its impact on the UK's data protection landscape.

Contents

The global state of play

Regulatory enforcement under GDPR soars

GDPR enforcement activity has risen sharply since the regulation came into effect.

In 2018, the year the GDPR came into force, there were just 19 penalties issued by EU DPAs, with Germany and Austria the nexus of activity. Total fines amounted to less than €600,000.

Enforcement really took off in 2019, with the number of fines increasing by a factor of seven to 143. Authorities in 24 EU countries issued fines in 2019 and 2020, compared with just eight in 2018.

In 2020, the number of GDPR-related fines rose 17 per cent to 168, and by the end of February 2021 a further 35 penalties had been handed out. If that level of activity were maintained to the end of the year, it would set another new high.

The size of the penalties issued by EU DPAs also increased significantly, with total fines more than doubling between 2019 and 2020 (123 per cent). To the end of February 2021, companies were punished to the tune of almost €28m, which again will break the previous record if the rate continues to the end of the year.

Spain brings the most cases; Italy levies the most fines

Spain is by far the most active EU jurisdiction for regulatory enforcement, with the AEPD issuing 110 separate GDPR-related penalties between 2018 and February 2021.

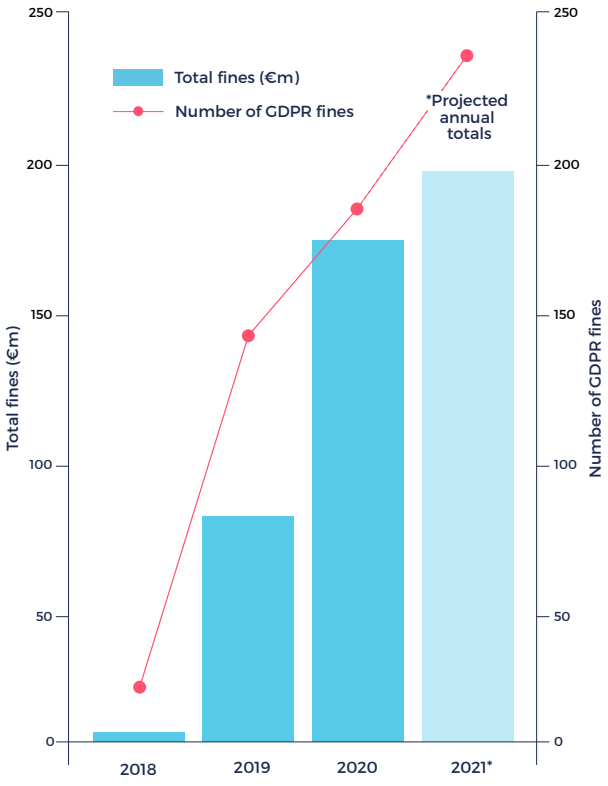
Italy's Garante, however, has handed out more fines (€70.9m) than any other EU authority, followed by France's Commission Nationale de l'Informatique et des Libertés (CNIL), German DPAs (which are organised regionally) and the UK Information Commissioner's Office (ICO). The latter levies the biggest individual penalties on average (€11m), including three major fines in 2020.

The sectors and infringements in the spotlight

The most heavily sanctioned industries are consumer, telecoms, healthcare and industrials.

The largest fines were reserved for companies whose GDPR violations affected the biggest number of data subjects; repeat offenders; and businesses deemed not to be co-operating with the relevant DPA. In Germany, there has been a crackdown on employee surveillance, while data security breaches are another driver of significant fines.

GDPR enforcement, 2018–2021



*Projections calculated from run rate at 26 February 2021

The global state of play

Trend for fines to be reduced

While GDPR-related penalties are rising, the fines being issued are not at the top end of the scale. The regulation gives EU DPAs the scope to fine companies up to 4 per cent of their annual group turnover, yet the actual amounts are significantly lower. Of the 50 biggest GDPR fines to date, only two (Ticketmaster UK and Notesbooksbilliger.de) represented more than 1 per cent of the company's global sales.

In addition, one of the most noticeable recent trends has been for fines to be reduced or even reversed by DPAs or the courts, with the UK ICO's cases against British Airways and Marriott two of the highest-profile examples.

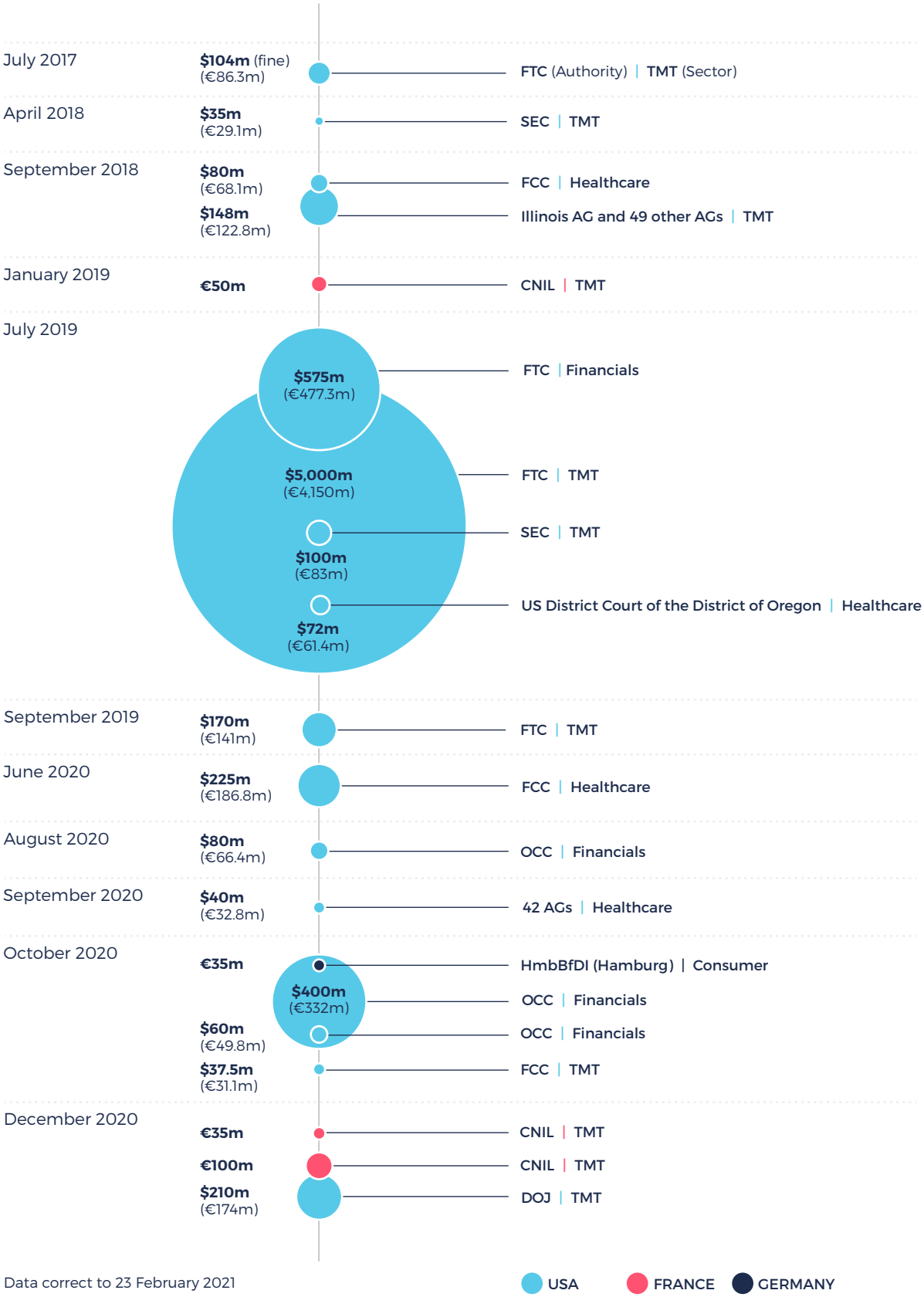
For more on fine reductions and reversals, see page 17.

Biggest fines globally originate in US

While the *level* of data protection enforcement in the EU has soared since the advent of the GDPR, the biggest data-related penalties globally originate in the US. Since 2018, nine of the 10 largest fines for data privacy breaches have all come from US authorities, with the Federal Trade Commission (FTC) the only regulator to hand out a 10-figure punishment. The US has no federal privacy regulation so fines are levied by a variety of authorities, including state attorneys general, the Office for Civil Rights, the FTC and the Department of Justice.

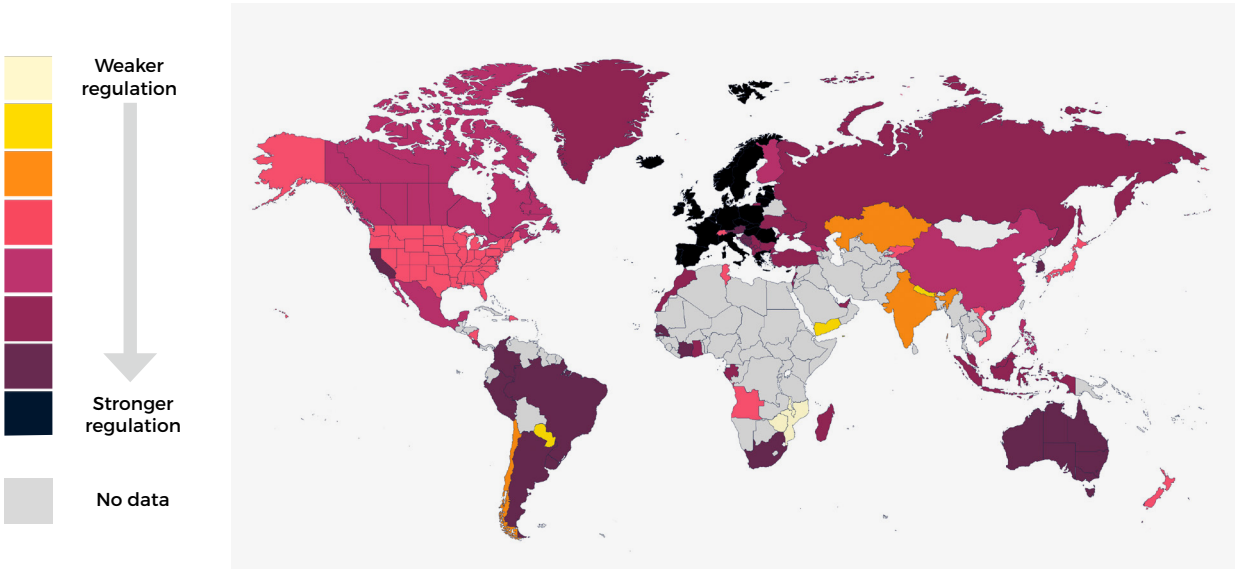
US companies – particularly in tech – are the most heavily sanctioned worldwide, with only one non-US company featuring among the 20 biggest penalties.

Top 20 data-related fines in Europe and North America, 2017–2021

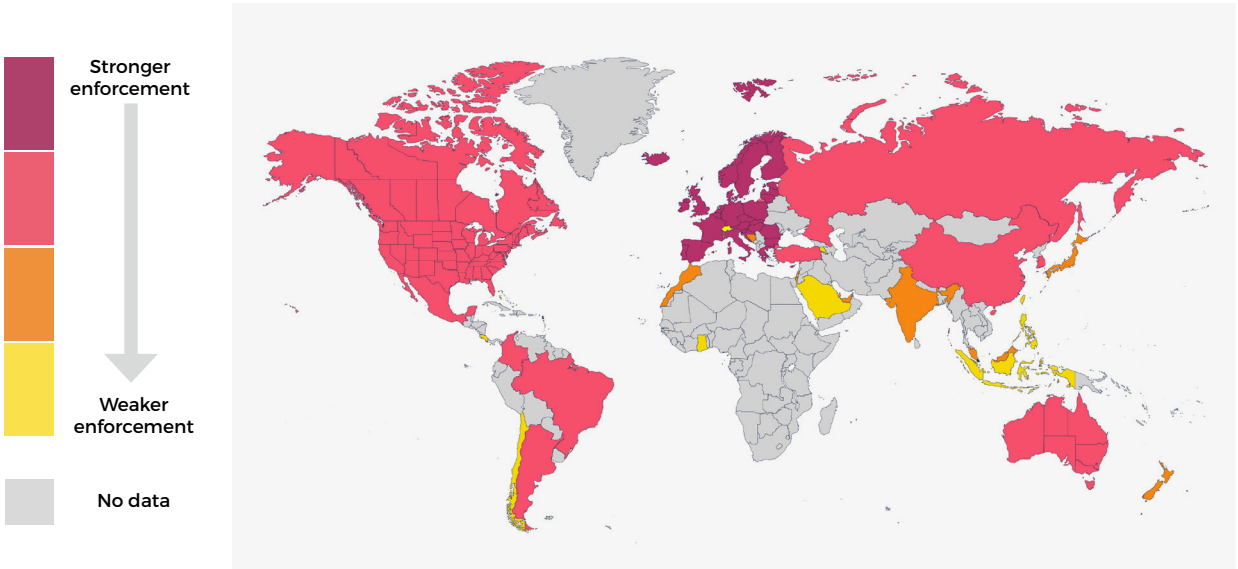


The global state of play

Privacy and cyber security regulation – the new normal



Data privacy – the most active regulators



Regional trends

United States

There is a long history of significant privacy penalties and settlements in the US (including the biggest ever at $5bn), with major penalties levied for over a decade.

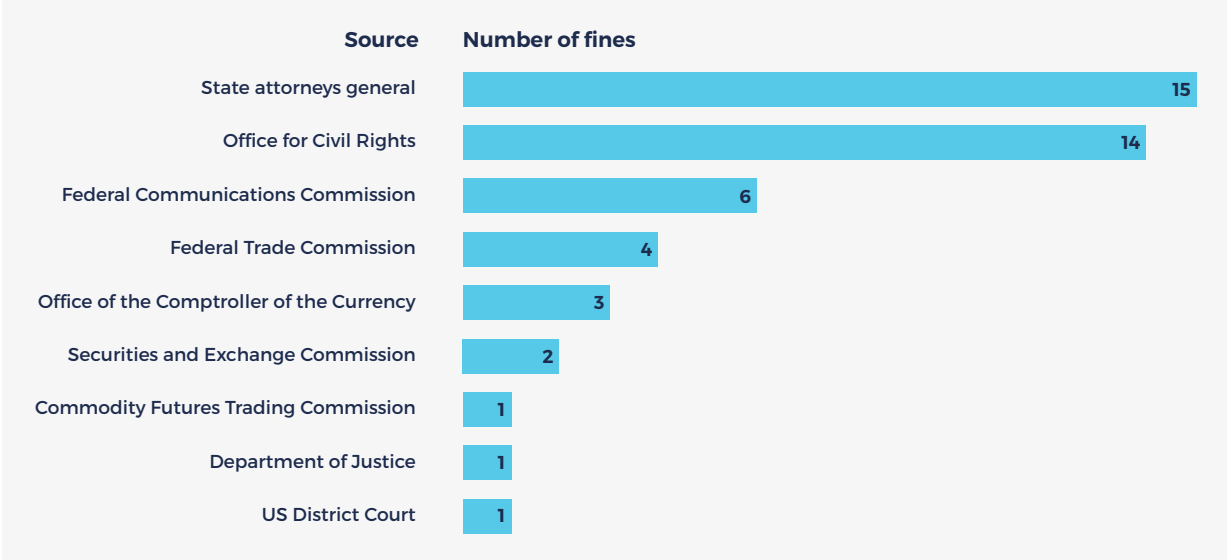
Penalties and settlements generally arise in three cases: data breaches; violations of special-purpose laws like the Health Insurance Portability and Accountability Act (HIPAA), the Gramm–Leach–Bliley Act (GLB) or the Children's Online Privacy Protection Act (COPPA); and violations of general consumer protection laws like the Federal Trade Commission Act. In addition, 2020 saw the first enforcement action by the New York State Department of Financial Services against an insurer based on that regulator's recently imposed cyber security regulations. Of note, the federal government agencies responsible for HIPAA enforcement relaxed some of its implementing regulations in response to the COVID-19 pandemic, which you can read about here.

One of the most active regulators in this space has been the Federal Trade Commission (FTC), which wields an assortment of enforcement tools against offending companies. Importantly, the Supreme Court is currently considering the scope of the FTC's power to require companies to compensate consumers monetarily as part of its order-making powers. The outcome of that question may have a major impact on privacy enforcement in the US.

Penalties are often reached by settlement between the authority and the alleged offender, while more individuals (particularly doctors) are fined for violations than is the case in Europe.

While the US has no generally applicable federal data privacy regulation (just the special-purpose laws mentioned above), the country's first fully fledged privacy law at the state level came into effect at the start of 2020. Enforcement of the California Consumer Privacy Act (CCPA) is still in its nascent stage; the California Attorney General has begun by issuing warning letters to various companies. The CCPA was extended in late 2020 via the California Privacy Rights and Enforcement Act (CPRA or CPREA), which will come into force in 2023 and bring California's privacy regime closer to GDPR. The CPRA will create the US's first true data protection authority and empowers it with an assortment of enforcement tools.

Where do the top 100 US fines originate?



Regional trends

Europe

In 2018, the first year of the GDPR, there was little enforcement activity outside Germany and Austria and the fines issued were relatively small.

In 2019, there was a significant uptick in activity, with more than 143 individual penalties issued. The size of the fines, however, only started to increase towards the end of the year, with the average penalty in 2019 hitting €630,000 (largely on the back of Europe's biggest data fine to date, a €50m sanction issued by France's CNIL). By 2020, the average GDPR fine had risen to more than €1m.

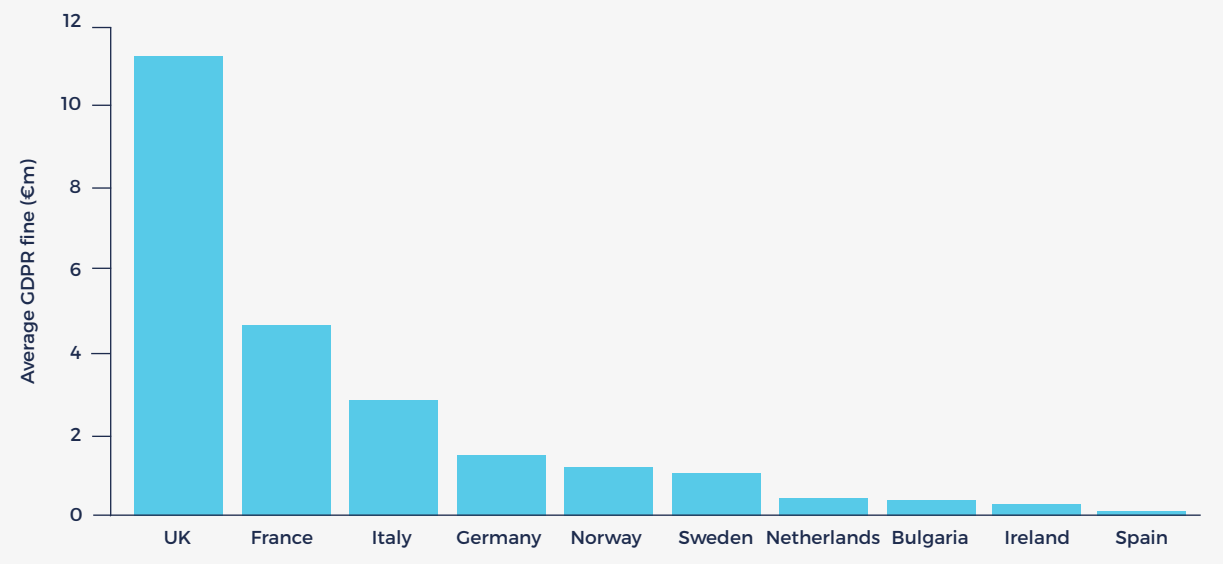
DPAs in the three biggest economies in Continental Europe – France, Italy and Germany – were active from the earliest days of the GDPR. Across the Channel, the UK ICO only really entered the fray in 2020 but since then has consistently gone after bigger cases, with its average fine of €11m more than double that of any other European country. Germany now appears to be following the UK's lead, with its average penalty rising €18m in 2020. Spain, too, has recently started to issue much larger penalties.

There is also a clear distinction emerging in the types of infringements pursued by different European DPAs – in the UK the ICO has focused on data breaches and security incidents; the German authorities have come down hard on employee surveillance; and Italy's Garante has taken a tough stance on general compliance and any lack of co-operation with its investigations.

The GDPR has served to align – to some extent – financial penalties across member states. EU DPAs co-operate to ensure that the regulation is applied consistently across the bloc and that enforcement action is effective, dissuasive and proportionate. At the same time, the GDPR gives individual DPAs the flexibility to develop their own methods of calculating penalties. For example, German authorities set fines based on the severity of the violation and do not necessarily consider whether the infringement is a first offence. The Italian authority, on the other hand, will first issue a warning and then a significant fine for failure to comply.

GDPR fines are handed out frequently, driven by the 'one-stop-shop' nature of the regulation's enforcement mechanism (whereby a DPA in one member state can act on behalf of the entire bloc), and the GDPR's narrow scope, which allows smaller fines to be issued for relatively minor offences.

Which member states issue the biggest average GDPR fines?



Regional trends

Direct marketing

Unlike their counterparts in the US, European authorities issue fewer fines in relation to direct marketing. EU member states have their own e-communications laws that cover direct marketing, cookies and spam, while the GDPR principles cover marketing more generally. Despite large fines being rare, there have been some significant penalties handed out, including from the CNIL which in December 2020 became the first EU authority to issue a major sanction for cookie violations. The EU is continuing to work on a new ePrivacy Regulation, which could see more enforcement in relation to electronic direct marketing in the future.

Asia

The data privacy landscape in Asia is evolving fast. There were several significant regulatory developments in 2020, with amendments to existing privacy laws in Singapore, Japan and Korea, and New Zealand's new Privacy Act coming into force. 2021 is expected to follow this trend, with further new laws and amendments in the pipeline in India, Indonesia, China and Hong Kong.

In particular, China's regulatory landscape is expected to undergo its most significant change since the advent of the country's Cyber Security Law (CSL) in 2017 with the introduction of a new Personal Data Protection Law.

Further reading

China's data privacy and security law: what to expect in 2021

India releases draft personal data protection bill

National trends

Germany

German DPAs come down hard on employee monitoring (issuing a €35m fine in 2020 and a €10.4m penalty in 2021). Germany is the third most active EU jurisdiction for GDPR enforcement actions (after Spain and Romania) and its courts have heard more individual damage claims for data protection violations than those of any other member state.

Hungary

Most fines are given anonymously.

Spain

Europe's most active GDPR enforcer. Spain's DPA, the AEPD, has repeatedly fined the same companies (particularly telcos) and has recently issued its first seven-figure penalties (€5m in December 2020 and €6m in January 2021), both to banks.

Italy

Italy's DPA has repeatedly targeted telcos, handing down individual fines of more than €10m to the country's three biggest operators in 2020. The Garante takes a tough line in cases of non-compliance with previous injunctions or warnings.

UK

The Information Commissioner's Office (ICO) has issued only four GDPR fines but they are among the biggest. The ICO has shown a particular interest in data breaches and security incidents resulting from insufficient technical or operational protections. Past decisions show that co-operation with the ICO can lead to significant fine reductions; two major penalties the authority issued in 2020 were both reduced significantly.

Sweden

Sweden's DPA is particularly strict in cases relating to unlawful access to health or patient data. It issued six times as many penalties in 2020 than 2019.

Hong Kong

Proposed revisions to Hong Kong's Personal Data (Privacy) Ordinance are currently being considered by the legislative council panel on constitutional affairs. These proposals include mandatory data breach notifications for incidents constituting a real risk of significant harm and enhanced sanctioning powers. The Personal Data Protection Commissioner would be given powers for the first time to issue direct administrative fines for breaches of the ordinance. The panel is exploring the feasibility of introducing an administrative fine linked to the annual turnover of the data user, within different turnover bands.

Singapore

Recent amendments to the Personal Data Protection Act, which were passed in November 2020 and which are being brought into force on a phased basis, include an increased financial penalty on organisations for breaches of the Personal Data Protection Act of the higher of up to 10 per cent of its gross turnover in Singapore or S$1m (previously capped at S$1m). The amendments also introduce new offences for individuals, including for the unauthorised disclosure or improper use of personal data and the unauthorised re-identification of anonymised information. These offences come with penalties that include a fine of up to S$5,000 or imprisonment of up to two years.

Legal trends

Why are companies being fined?

Direct marketing

Focus for: US

A significant number of US data privacy fines relate to direct marketing, which includes e-marketing, telemarketing, SMS/MMS communications and postal marketing. The penalties in question generally relate to spam or cookie consent.

Data breaches/data security

Focus for: UK and US

Enforcement authorities are issuing major fines to companies that suffer data breaches or are deemed to lack adequate data security measures.

The UK ICO has focused heavily on pursuing data breaches (eg the British Airways and Marriott cases in 2020), while US authorities have also handed out significant penalties (eg Dish Network, which was fined the equivalent of more than €170m by multiple agencies in 2020). Data breaches often lead to further financial exposure, particularly group action litigation by the individuals affected; these claims are often brought because of a general perception that a data breach must be the result of the business not fulfilling its data security obligations. However, the increasing sophistication of hacking attacks means even the best-prepared companies are vulnerable. To read our guidance on how to protect your business and respond to a data crisis, including litigation, request a copy of our report Anatomy of a Data Breach: what really happens in a global cyber crisis?

Protecting employee data

Focus for: Germany

There is an emerging trend for DPAs in Europe to come down hard on employee surveillance, particularly in Germany where several big fines have been issued.

In 2020, the Hamburg DPA fined a major retailer €35m for unlawfully collecting and storing health information on employees at its customer service centre in Nuremberg.

In response to the rise in homeworking driven by the COVID-19 pandemic, many countries have issued specific guidance on the dos and don'ts of employee monitoring.

Further reading

WorkLife 2.0 –'my algorithm boss is watching me'
How to manage data protection requirements in times of COVID-19
Unblurring videoconferencing legal risks

Health data

Focus for: US and Sweden

Health information is considered a special category of data and requires a higher level of protection.

As a result, the way companies handle health data is closely scrutinised, with authorities looking at issues such as how it's transferred and who has access to it.

There is a particular focus on health data in the US and Sweden, where big fines are common.

In the US, the Department of Health and Human Services' Office for Civil Rights (OCR) is a nexus of enforcement. In Sweden, hospitals and health insurance companies have been fined for giving staff unlawful access to individuals' health information.

Health data is in focus as a result of the COVID-19 pandemic, playing as it does a central role in contact tracing apps.

Further reading

Contact tracing apps: a three-part global series

Legal trends

Brexit

While the UK is no longer treated as part of the EU following the end of the Brexit transition period, the EU GDPR has been largely retained in UK law (at least for now). A major factor in the UK/EU negotiations was the GDPR's ban on sending personal data out of the EEA to countries that do not have 'adequate' data protection laws (with certain carve-outs, eg where the data is protected by contract). There was a concern that data flows from the EEA to the UK would be affected, as the EU had not officially declared the UK's law to fall into this category. This issue was partially addressed in the EU/UK Trade and Cooperation Agreement (TCA), which governs the relationship between the EU and the UK. The TCA includes a new six-month transitional period for EEA/UK data flows, giving the EU more time to assess the UK's 'adequacy'. If the European Commission decides that the UK does *not* have an adequate level of data protection, businesses will need to use additional safeguards, such as putting in place the model data export contracts approved by the EU.

Following Brexit, many multinational businesses will now be subject to both the UK and EU data regimes. Among other things, this means considering who their relevant regulator will be and whether they need local representatives in either or both jurisdictions. These issues should be addressed sooner rather than later; if a business suffers a data breach it must notify relevant regulators quickly, so multinational enterprises need to be joined up.

Further reading

Data protection under the EU-UK Trade Cooperation Agreement

Brexit Zone: Your data

Litigation and damages claims

Data-related litigation is a growing risk for businesses, and not just in the US. We have analysed almost 40 damages claims brought in Europe since 2018 and identified some key trends below.

Germany

Germany has the highest number of individual data-related damages claims in Europe, with more than 20 cases heard since 2018.

The highest sum awarded to an individual data subject was €5,000 for a breach of data subject access rights (Article 15 GDPR). The court ruled the defendant had failed to provide complete information and to provide it on time.

In another case, a data subject was awarded €4,000 after their psychotherapist forwarded on sensitive data. This was deemed a breach of Article 9 GDPR, with the court imposing a high fine as a deterrent.

Austria

The Austrian courts heard nine cases between 2018 and 2020, including seven in 2019.

Austria's Supreme Court handed down the country's highest damages award (€2,400) in a case involving employee surveillance. The court heard the plaintiff was allowed to use a company vehicle but was not aware it was fitted with a GPS tracker that did not differentiate between private and work journeys. After the employee was fired, they claimed damages for infringement of privacy.

Netherlands

The Dutch courts have awarded damages to data subjects ranging from €250 to €500.

The highest award relates to a plaintiff whose Freedom of Information request was shared with other public authorities without the documents being anonymised. The court used Article 82 GDPR in conjunction with Article 6:106 of the Dutch Civil Code, holding that the misuse of the data was sufficient to justify non-material damages.

UK

The UK courts have considered a number of group actions brought in relation to breaches of data protection law.

In April 2020, the Supreme Court issued a decision in a group action brought against the Morrisons supermarket chain. A large group of employees had sued Morrisons after a colleague published information about them online, but the court found that Morrisons was not vicariously liable for the employee's actions. For more details on the decision, see here.

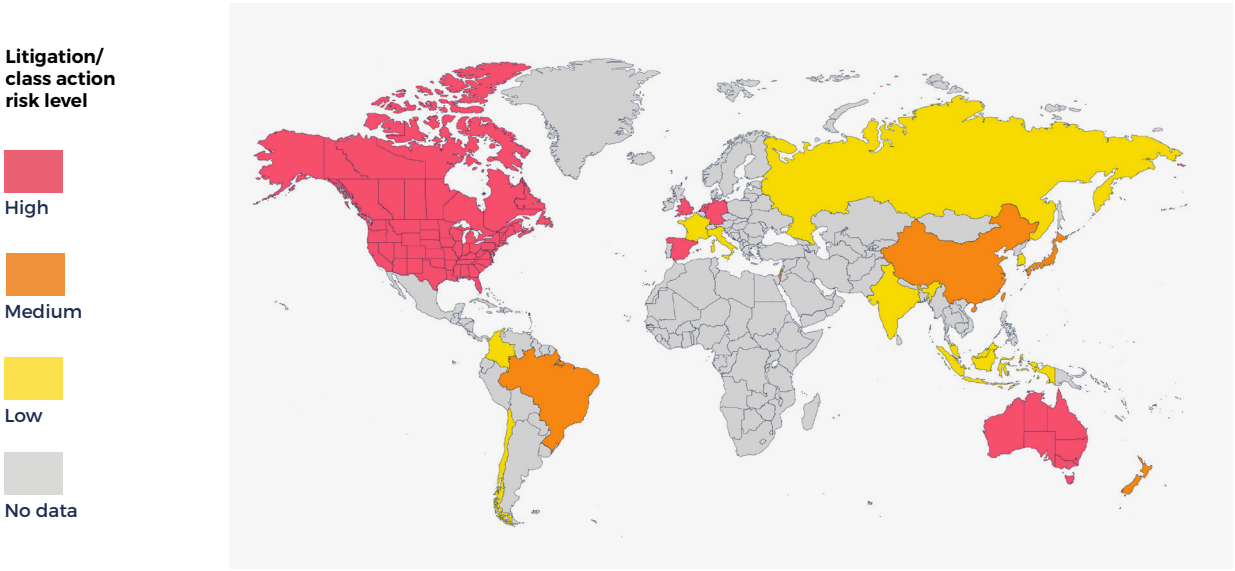
A significant UK group action is also expected to be heard by the Supreme Court in 2021. If the court decides in favour of the claimant, the case could open the floodgates to group data privacy claims. In particular, the court will determine whether damages can be awarded for 'loss of control' of data even if there is no resulting *financial* loss.

United States

Most data privacy cases in the US are class actions that seek monetary damages. There is an emerging perception in the US that if a data breach has occurred, some failure of technical or organisational measures must have been involved. This in turn is seeing more plaintiffs join class actions in search of damages. In some cases, class actions have been filed just weeks after a data breach has occurred, with plaintiffs not waiting to see if there is any regulatory enforcement. While the US courts have dismissed many claims early on so far, this is certainly an area to watch for the future.

Litigation and damages claims

Litigation/class action heat map – active class action regimes



Fine reductions and reversals

In recent years there has been a trend towards fines being reduced or even reversed, by either the courts or the DPAs themselves.

In some cases, the courts have stepped in to reduce fines deemed unreasonably high, or because the DPA in question had misinterpreted or misapplied the law.

Where DPAs are concerned, there are a number of factors that contribute to fines being cut:

- prompt notification and communication with the relevant authorities;
- co-operation during the investigative process;
- the development of an action plan to show how the problem will be solved and/or a commitment to increasing the level of data protection;
- voluntary payment (only Spain);
- external factors such as the financial impact of the COVID-19 crisis (eg the UK ICO cut Ticketmaster UK's fine by £500,000); and
- reassessment of the underlying facts.

For further insights on how authorities set fines and how to respond to a regulatory investigation, please request a copy of our report Anatomy of a Data Breach: what really happens in a global cyber crisis?

Year	Country	Authority	Company	Intended fine	Actual fine
2020	UK	ICO	British Airways	£183m	£20m (includes COVID reduction)
2020	UK	ICO	Marriott International	£99.2m	£18.4m (includes COVID reduction)
2020	UK	ICO	Ticketmaster UK	£1.75m	£1.25m
2020	Netherlands	AP	Voetbal.tv	€575,000	€0 (fine overturned by the District Court Midden-Nederland)
2019	Germany	BlnBDI (Berlin)	Deutsche Wohnen SE	€14.5m	€0 (dismissed by the Berlin Regional Court on 23 February 2021)
2019	Germany	BfDI	1&1 Telecom GmbH	€9.6m	€900,000
2019	Austria	DSB	Austria Post	€18m	€0 (fine overturned by the Federal Administrative Court)
2019	Germany	HmbBfDI (Hamburg)	Kolibri Image	€5,000	€0 (fine overturned by the court)

Data compiled from a variety of public databases and subscription services and correct to 26 February 2021.

freshfields.com