A REPORT BY DLA PIPER'S CYBERSECURITY AND DATA PROTECTION TEAM

DLA Piper GDPR fines and data breach survey: January 2021

DLA PIPER

DLA Piper GDPR fines and data breach survey: January 2021

The EU General Data Protection Regulation (GDPR) has applied across the European Union since 25 May 2018. In what was an extraordinary year for many reasons, Europe's data protection supervisory authorities and those they regulate have been grappling with the tough requirements imposed by GDPR and the legal questions it leaves unanswered.

With thanks to the many different contributors[1] and supervisory authorities who make this report possible, our third annual survey covers key GDPR metrics across the European Economic Area (EEA)[2] and the UK[3] since GDPR first applied and for the year to 27 January 2021.

"Regulators have been testing their new powers this year, issuing EUR158.5m (USD193.4m / GBP142.7m)[4] in fines since 28 January 2020. But they haven't had it all their own way, with some notable successful appeals and large reductions in proposed fines."

1 This publication has been prepared by DLA Piper. We are grateful to Batliner Wanger Batliner Attorneys at Law Ltd., Glinska & Miskovic, Kamburov & Partners, Kyriakides Georgopoulos, LOGOS, Mamo TCV Advocates, Pamboridis LLC, Schellenberg Wittmer Ltd and Sorainen for their contributions in relation to Liechtenstein, Croatia, Bulgaria, Greece, Iceland, Malta, Cyprus, Switzerland, Estonia, Latvia and Lithuania respectively.

2 The EEA includes all 27 EU Member States plus Norway, Iceland and Liechtenstein.

3 The UK left the EU on 31 January 2020. The UK has implemented GDPR into law in each of the jurisdictions in the UK (England, Northern Ireland, Scotland and Wales), which as at the date of this report is the same in all material respects as GDPR.

4 In this report we have used the following exchange rates: EUR1 = GBP0.9 / USD1.22.

Summary and key findings

Significant increase of breach notifications

It has been more than two and half years since GDPR first applied on 25 May 2018. For the period from 28 January 2020 to 27 January 2021 there were, on average, 331 breach notifications per day (a 19% increase on the previous year average of 278 notifications per day), so the current trend for breach notifications continues to see double digit growth.

Testing new powers and successful appeals

The supervisory authorities responsible for enforcing GDPR[5] have not been idle; some notable fines have been imposed relating to a wide variety of infringements. The UK left the EU on 31 January 2020. The UK's supervisory authority, the Information Commissioner's Office (ICO), has, however, been active, issuing several large fines.

Regulators have been testing their new powers this year, issuing a total of EUR158.5m (USD193.4m / GBP142.7m)[6] in fines since 28 January 2020. But they haven't had it all their own way, with some notable successful appeals and large reductions in proposed fines.

The Austrian supervisory authority had a bad end to the year when its headline EUR18m (USD22m / GBP16.2m) fine imposed on Austrian Post was overturned by the Austrian Federal Court on 2 December 2020. Similarly, the two fines issued by the ICO in the UK were reduced from the originally proposed GBP189.39m (EUR210.4m / USD256.7m) and GBP99.3m (EUR110.3m / USD134.6m) to GBP20m (EUR22.2m / USD27.1m) and GBP18.4m (EUR20.4m / USD24.9m) respectively. In percentage terms, the reductions secured were 90% and 80% of the originally proposed fines. The ICO noted in its final penalty notices that the originally proposed fines had been discounted in part in light of the financial hardship caused by COVID-19. Nevertheless, it evidently pays to appeal and to mount robust challenges to proposed regulatory sanctions.

Highest individual fine league table

#1

France's data protection supervisory authority, the CNIL, retains pole position, having fined Google Inc EUR50m (USD61m / GBP45m) in January 2019 for breaching GDPR transparency requirements, and for failing to have an adequate legal basis for processing in relation to personalised advertising (breach of Articles 6, 12 and 13 GDPR).[7]

#2

The Hamburg data protection supervisory authority is in second place, having fined a global retailer EUR35.26m (USD43m / GBP31.7m) in October 2020 for failing to have a sufficient legal basis for processing (breach of Articles 5 and 6 GDPR).

#3

In third place, Italy's data protection supervisory authority, the Garante, fined a telecommunications operator EUR27.8m (USD33.9m / GBP25m) in January 2020 for a number of breaches of GDPR, including breaches relating to transparency obligations, failing to have a sufficient legal basis for processing personal data, and inadequate technical and organisational measures, and breach of the principle of privacy by design (breach of Articles 5, 6, 17, 21 and 32 GDPR).

5 All references in this report to infringements or breaches of GDPR are to findings made by relevant data protection supervisory authorities when issuing fines. In a number of cases, the entity subject to the fine has disputed these findings and the penalty notices are subject to appeal. DLA Piper makes no representation as to the validity or accuracy of the findings made by relevant supervisory authorities.

6 Not all supervisory authorities publish details of fines. Some treat them as confidential. Our report is, therefore, based on fines that have been publicly reported or disclosed by the relevant supervisory authority. It is possible that other fines have been issued on a confidential basis.

7 The CNIL was in the news again in December 2020, having imposed another fine on Google entities for a total of EUR100m. However, these fines related to alleged violations of e-privacy laws rather than GDPR infringements, so are not included in the metrics in this report.

In the rankings of the total value of all GDPR fines issued to date, the data protection supervisory authority in Italy tops the table, having imposed fines totalling EUR69,328,716 (USD84,581,033 / GBP62,395,844). The data protection authorities in Germany and France are in second and third place with fines totalling EUR69,085,000 (USD84,283,700 / GBP62,176,500) and EUR54,436,000 (USD66,411,920 / GBP48,992,400) respectively.

Total amount of fines

Last year, the total (reported) fines for the full 20-month period since the introduction of GDPR on 25 May 2018 was just over EUR114m (USD139m / GBP103m), which we noted in our previous report was quite low, given that supervisory authorities enjoy the power to fine organisations up to 4% of their total worldwide annual turnover for the preceding financial year. The total (reported) fines since 25 May 2018 has more than doubled to just over EUR272m (USD332m / GBP245m), with EUR158.5m (USD193.4m / GBP142.7m) over the last 12 months alone, a 39% increase on the previous 20-month period since GDPR came into force.

Many open legal questions

There are many open legal questions relating to GDPR, including whether fines should be assessed against the consolidated global revenue of the organisation being fined, or just against the revenue of the specific legal entity responsible for the infringement.

The clear intent of the non-legally binding recitals in GDPR supports the former broad interpretation, which is also supported by the influential European Data Protection Board.[8] However, the legally binding articles of GDPR conflict with the recitals and appear to limit the assessment of fines to the revenues of the specific entity being fined. This is a critical point of interpretation, as it potentially significantly limits the maximum fine that regulators can impose under GDPR.

It is also open to interpretation whether fines for breach of Article 5(1)(f) and Article 32 (the integrity and confidentiality principle and the related requirement to ensure the security of processing personal data) should be capped at 2% or 4% of total worldwide annual turnover. Having considered this issue when imposing two headline-grabbing fines last year, the UK ICO concluded in its penalty notices that the higher 4% maximum fine applied to breaches of security. That said, this is far from being settled law, and we expect the point to be argued in future appeals of fines, given the significant amounts involved.

The many open legal questions and uncertainties in the interpretation and application of GDPR perhaps explain, in part, why the fines imposed to date by supervisory authorities have been at the lower end of the scale of potential maximum fines.

As was the case in last year's report, fines certainly aren't the only exposure for organisations that fall short of GDPR's exacting requirements. The continuing fallout of the *Schrems II*[9] judgment, handed down in July 2020 by Europe's highest court, is a reminder of the broad range of other sanctions supervisory authorities can impose. Maximillian Schrems has, through his organisation My Privacy is None of Your Business, issued 101 complaints to lead supervisory authorities.[10] These complaints demand, in addition to fines, the immediate suspension of alleged illegal transfers of personal data from the EU to third countries. There is also an increased risk of "follow-on" compensation claims, including US-style "opt-out" class action in a number of EU Member States and the UK, fuelled by billions of euros invested in litigation funds looking for claims to support.

8 The European Data Protection Board is made up of representatives from all 27 EU Member States and the European Data Protection Supervisory Authority. The supervisory authorities of the EFTA EEA States are also members with regard to the GDPR-related matters (without the right to vote or be elected as chair or deputy chairs).

9 *Data Protection Commissioner* v *Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18).

10 See https://noyb.eu/en/101-complaints-eu-us-transfers-filed

Commentary

Some things stay the same

A recurring theme of the three DLA Piper GDPR reports issued to date is that there has been little change at the top of the tables regarding the total number of data breach notifications made since GDPR came into force on 25 May 2018 and during the most recent full year from 28 January 2020 to 27 January 2021.

The Netherlands, Germany and the UK retain the top three rankings in both tables, albeit that Germany now takes pole position. There has been some movement at the top of the weighted breach notifications per 100,000 capita table: Denmark now takes the top spot (up three places from last year's report), with the Netherlands and Ireland in second and third places. Italy continues to sit near the bottom of the population-weighted breach notification table. With a population of more than 62 million people, Italy has recorded only 3,460 breach notifications since GDPR came into force on 25 May 2018, ranking second from last on the population-weighted breach notification table.

The story regarding fines is similar, with notable variations in the total value of fines imposed by each country surveyed. These wide variations illustrate that, although data protection laws in the EEA and the UK all derive from GDPR, the compliance culture of organisations and the interpretation and enforcement practice of the different data protection supervisory authorities varies significantly. This regulatory uncertainty is particularly challenging for multinational organisations with operations in multiple countries. It is also challenging for their insurers, compounded by the legal uncertainty surrounding whether GDPR fines can be recovered under an insurance policy.[11]

Evolving enforcement trends

Despite the overall inconsistency in approaches among the countries surveyed, some common enforcement trends are evident.

Failure to comply with the transparency principle

First, many supervisory authorities have prioritised the enforcement of violations of the lawfulness, fairness and transparency principle (Article 5(1)(a) GDPR). Early enforcement demonstrates that supervisory authorities are setting a high bar to meet the information disclosure requirements of GDPR, fining controllers with overly complex privacy notices and notices deemed to be insufficiently granular, inaccurate or incomplete.

For anyone who has had to draft privacy notices, transparency is a conundrum. Include too much detail and it may not be understandable to your audience, breaching GDPR's transparency principle. Include too little and you risk being sanctioned for providing incomplete or inaccurate information. A layered approach is a potential solution, though care is required: controllers have also been fined for having "fragmented" information where users are required to navigate and cross-check multiple different privacy notices. For some processing, the challenge is simply that the complexity of the processing and data flows is extremely difficult to explain in lay terms, particularly given the reality that, save for data protection lawyers, very few consumers ever read privacy notices.

11 See the third edition of *The Price of Data Security* guide to the insurability of GDPR fines across Europe, compiled by global insurance broker AON and DLA Piper.

Failure to demonstrate a lawful basis to process

Failure to demonstrate a lawful basis to process is another emerging trend in the early GDPR fines. In some cases, the supervisory authority concluded there simply could not be any lawful basis for the processing in question. In others, although a lawful basis was in theory available, the controller failed to demonstrate evidence of the lawful basis, underlying the importance of effective governance and accountability. Several fines have been imposed for failures to obtain GDPR standard consent or for seeking to rely on invalid consent.

Tackling unlawful processing requires a combination of good data mapping in comprehensive and accurate records of processing; good data protection governance, to ensure there is a lawful basis for all processing and that it is documented to demonstrate accountability; and good privacy notices that clearly set out the lawful basis for each processing activity. In combination, this is a sizeable task, so it is sensible to apply a risk-based approach with more time and attention given to higher-risk processing activities, using available guidance defining high-risk processing for the purposes of data protection impact assessments.[12]

Failure to implement appropriate security measures

Over the last 12 months, some of the larger data breach-related fines have been imposed. GDPR requires organisations to implement "appropriate" technical and organisational measures to ensure a level of security appropriate to the risks of processing taking into account the ever-changing state of the art and the costs of implementation. The early GDPR fines are beginning to provide some welcome detail on what may constitute "appropriate" measures depending on the context. In different situations, the omission of one or more of the following measures has been specifically called out as potentially contributing to a breach of Article 32 and the related Article 5(1)(f) GDPR:

- monitoring privileged user accounts
- monitoring access to and use of databases storing personal data
- implementing "server hardening" techniques to prevent access to administrator accounts
- encryption of personal data, particularly more sensitive personal data
- use of multi-factor authentication to prevent unauthorised access to internet-facing applications
- strict access controls for applications on a needs basis, with prompt removal of access when no longer required
- regular penetration testing
- not storing passwords in plain-text unencrypted files (known as hardcoding)
- logging failed access attempts
- carrying out manual code reviews to check personal data is not being logged where it should not be
- processing payment card information in accordance with the PCI DSS Standard

In light of this new guidance, organisations may wish to consider the appropriateness of these measures in the context of their respective efforts to protect personal data and to consider documenting the basis for the adoption (or omission) of particular measures to address accountability.

12 See EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01.

Breach of the data minimisation and data retention principles

The risk of harm for data subjects, and therefore the follow-on risk of fines and other sanctions for organisations processing their personal data, is often compounded where there are breaches of the data minimisation principle (Article 5(1)(c)) or the storage limitation principle (Article 5(1)(e)). Processing too much data or over-retention can compound harm arising from illegal processing or data breaches. During the two decades before the introduction of GDPR, a combination of relatively light regulation of personal data and an exponential growth in the amount of personal data processed and stored by organisations has created a legacy compliance challenge for organisations. Finding, classifying and then retaining or deleting personal data across multiple legacy applications is a resource-intensive, time-consuming and complex task. The task is further complicated by much of legacy data being unstructured and stored in old systems and applications that either cannot or do not easily support the secure deletion of personal data. Despite these complexities, data protection supervisory authorities have shown little leniency when enforcing these core principles. Notably, in October 2019, Deutsche Wohnen SE was fined EUR14.5m (USD17.7m / GBP13m) by the Berlin Commissioner for Data Protection and Freedom of Information for, among other things, breach of the data minimisation and storage limitation principles. More recently, the French CNIL fined the online shoes retail company SPARTOO SAS EUR250,000 (USD305,000 / GBP225,000) for, among other things, breaches of these principles. Given the size of the task, careful planning is required and interim controls may be necessary pending the implementation of full deletion capabilities to reduce the risk of harm to data subjects. Another lesson from these early fines is that doing nothing is a risky option.

Data transfer requirements: a notable omission

One notable omission from the list of infringements giving rise to GDPR fines – or at least any sizeable fine – is breach of the Articles in Chapter V GDPR relating to the transfer of personal data to third countries and international organisations. It is likely to take a while for the ramifications of the *Schrems II* judgment of the CJEU to filter through to enforcement practice. For the large majority of organisations relying on standard contractual clauses to legitimise exports of personal data from the EEA and UK to third countries, there is a significant amount of work to do to map and carry out transfer impact assessments,[13] followed by implementing updated standard contractual clauses when the recently issued drafts have been finalised by the Commission.[14]

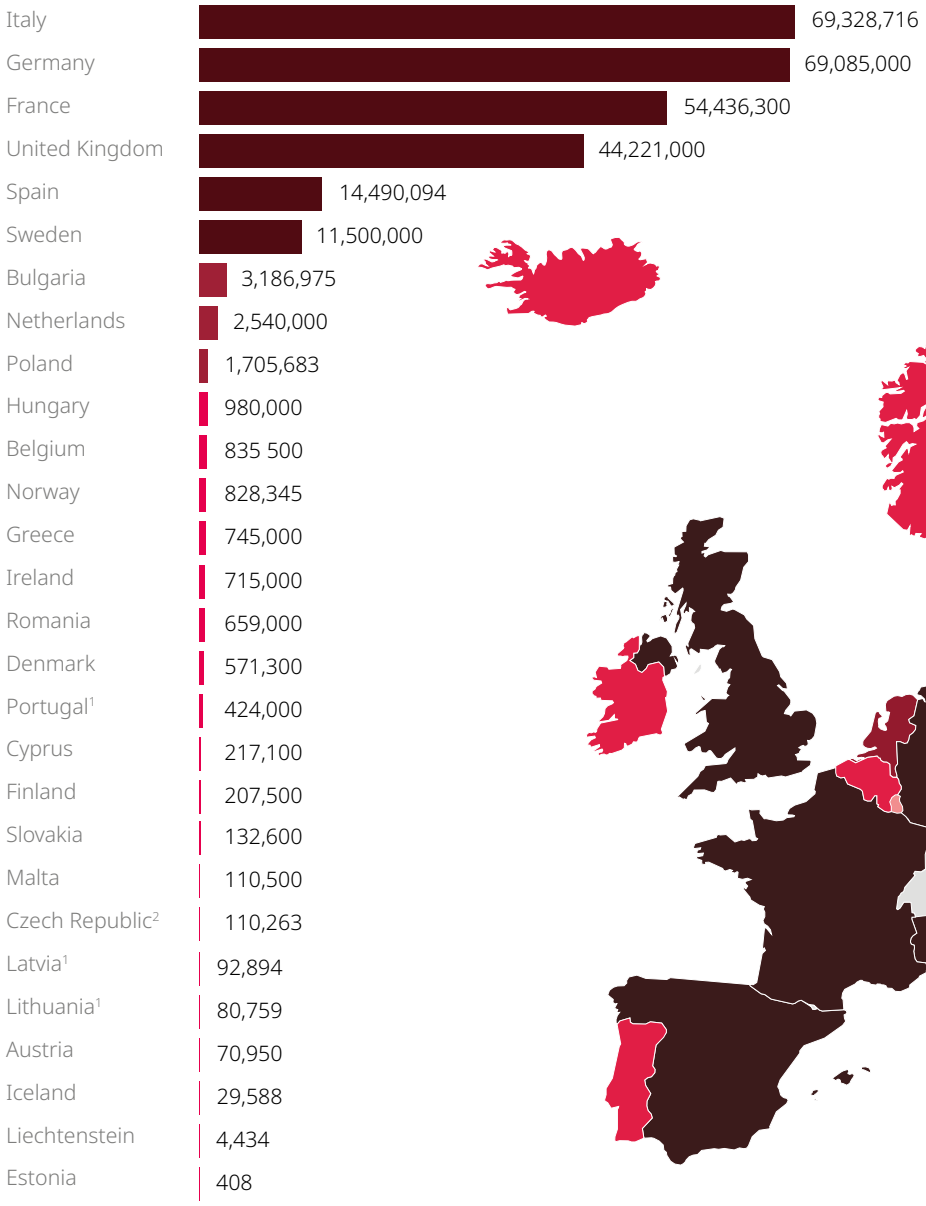
"One of the many open legal questions is whether fines should be assessed against the consolidated global revenue of the organisation being fined or just the revenue of the specific legal entity responsible for the infringement."

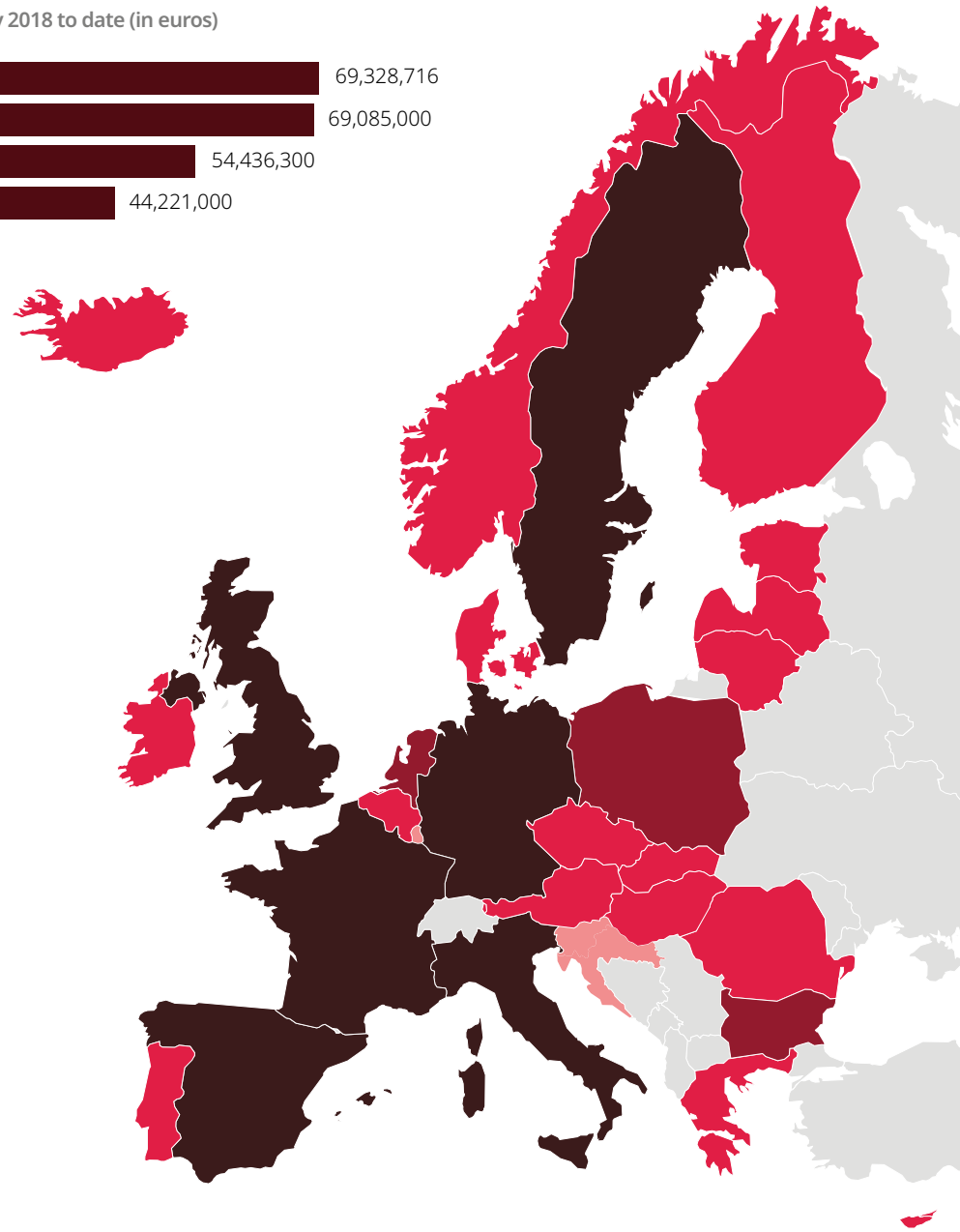
13 DLA Piper has developed the DLA Piper Global Data Transfer Methodology to support transfer impact assessments. Please get in touch with your usual DLA Piper contact or email dataprivacy@dlapiper.com for more details.

14 See the European Commission's Draft implementing decision and Anex – Ares(2020)6654686, available on the ec.europa.eu website.

Report

Total value of GDPR fines imposed from 25 May 2018 to date (in euros)

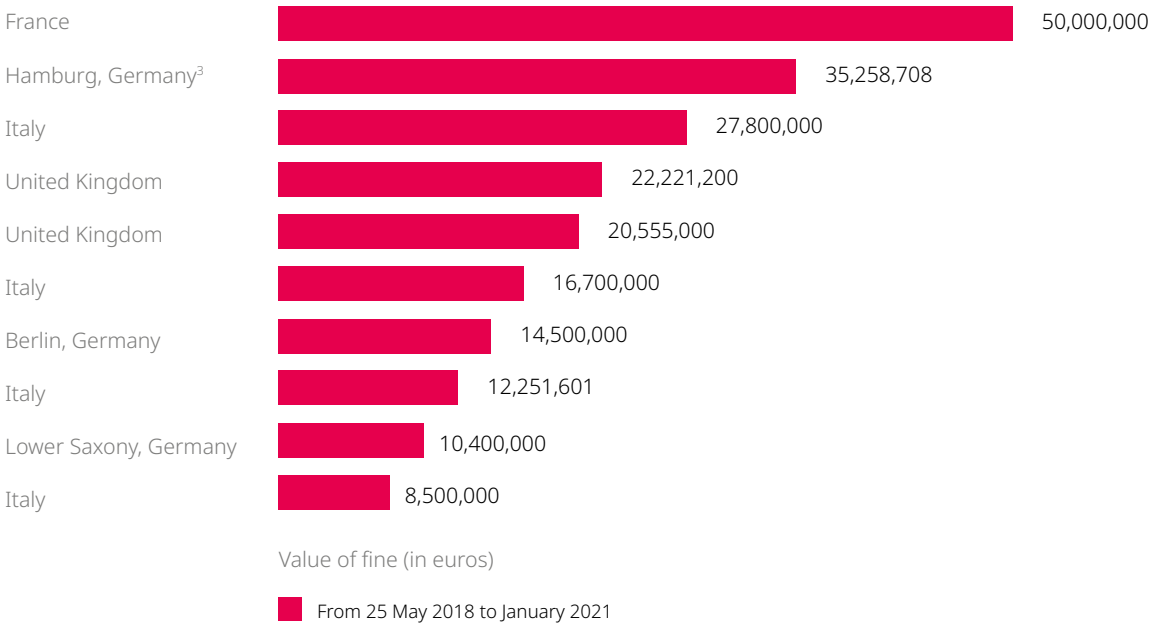




1 Data available only to the end of 2019, so the figure reported may be lower than the actual aggregate value of fines to date.

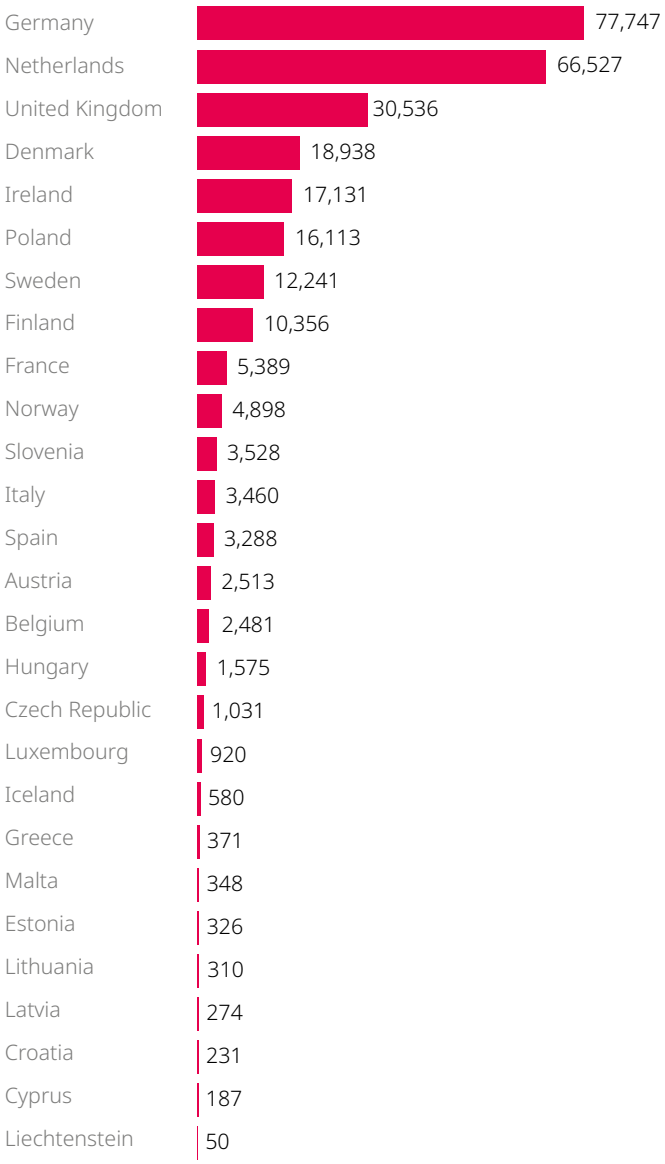
2 The Czech Republic supervisory authority confirmed that the figures reported last year may have included some non-GDPR fines, hence the lower figure reported this year.

Top ten largest fines imposed to date under GDPR



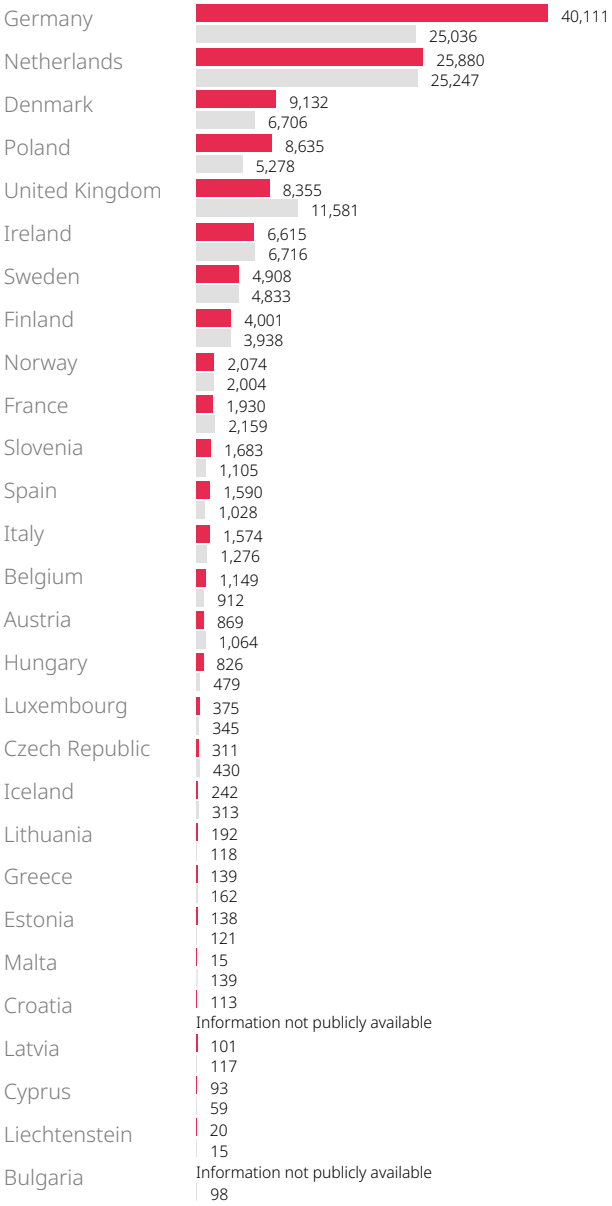
3 Germany has 16 different state data protection supervisory authorities, plus a federal supervisory authority.

Total number of personal data breaches notified per jurisdiction for the period from 25 May 2018 to 27 January 2021 inclusive*



From 25 May 2018 to 27 January 2021

Number of data breaches notified per jurisdiction between 28 January 2020 and 27 January 2021 inclusive*

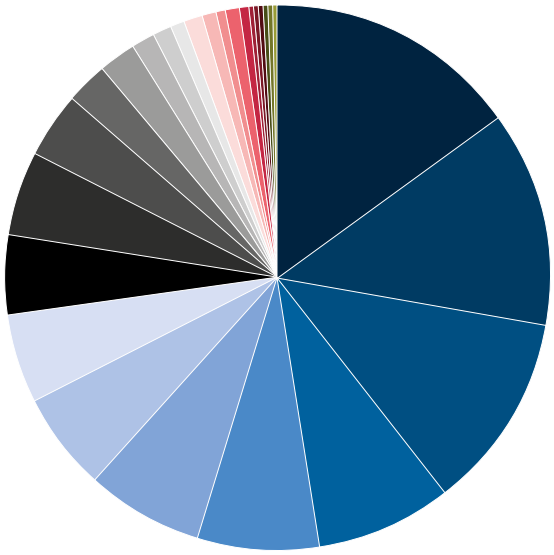


From 28 January 2020 to 27 January 2021

From 28 January 2019 to 27 January 2020

*Not all the countries covered by this report make breach notification statistics publicly available, and many provided data for only part of the period covered by this report. We have, therefore, had to extrapolate the data to cover the full period. It is also possible that some of the breaches reported relate to the regime before GDPR.

Per capita country ranking of breach notifications*	Number of data breaches per 100,000 people for the period 25 May 2018 to 27 January 2021	Change compared to last year's ranking
Denmark	155.6	+3
Netherlands	150	-1
Ireland	127.8	+1
Slovenia	80	+3
Finland	71.8	No change
Iceland	69.1	-2
Luxembourg	59.6	-1
Liechtenstein	51	+1
Germany	50	+2
Sweden	48.1	-2
Norway	37.9	-1
Malta	23.8	No change
Poland	22.6	+1
United Kingdom	12.7	-1
Estonia	11.2	+1
Austria	9.8	-1
Belgium	9.8	No change
Hungary	8.5	+1
Cyprus	7.3	+1
Lithuania	7	+1
Latvia	5.4	-3
Spain	3.2	+2
Czech Republic	2.9	-1
France	2.8	-1
Croatia	2.7	Information not publicly available
Italy	2.5	-1
Greece	1.3	No change



*Per capita values were calculated by dividing the number of data breaches reported by the total population of the relevant country multiplied by 100,000. This analysis is based on census data reported in the CIA World Factbook (July 2020 estimates).

Additional resources

The DLA Piper global cybersecurity and data protection team of more than 180 lawyers has developed the following products and tools to help organisations manage their data protection and cybersecurity compliance. For more information, visit dlapiper.com or get in touch with your usual DLA Piper contact.

DLA Piper Data Protection Laws of the World

Our online *Data Protection Laws of the World* handbook offers a succinct overview of a range of areas of data protection law, such as breach notification requirements and enforcement, for over 90 jurisdictions, with the ability to compare and contrast laws in different jurisdictions in a side-by-side view. The handbook also features a visual representation of the level of regulation and enforcement of data protection laws around the world.

DLA Piper Global Data Transfer Methodology

In response to the *Schrems II* judgment of Europe's highest court, we have designed a standardised data transfer methodology to help data exporters and importers logically assess the safeguards available when transferring personal data to particular third countries and whether they are adequate. The methodology includes a five-step assessment process, comprising a proprietary scoring matrix and weighted assessment criteria to help manage effective and accountable decision-making. It comprises a suite of legal equivalence assessments of common importing third countries.

DLA Piper Privacy Matters Blog

We have a dedicated data protection blog, *Privacy Matters*, where members of our global team post regular updates on topical data protection, privacy and security issues and their practical implications for businesses. Subscribe to receive alerts when a new post is published.

DLA Piper Data Privacy Scorebox

Our Data Privacy Scorebox helps to assess an organisation's level of data protection maturity. It requires completing a survey covering areas such as storage of data, use of data, and customers' rights. A report summarising the organisation's alignment with 12 key areas of global data protection is then produced. The report also includes a practical action point checklist and peer benchmarking data.

DLA Piper Notify: Data Breach Assessment Tool

We have developed an assessment tool, known as Notify, that allows organisations to assess the severity of a personal data breach, using a methodology based on objective criteria from official sources to determine whether or not a breach should be notified to supervisory authorities and/or affected individuals.

The tool automatically creates a report that can be used for accountability purposes as required by GDPR.

DLA Piper and AON: The Price of Data Security

We have partnered with global insurance and reinsurance broker AON for the third year running for the updated edition of *The Price of Data Security*, a guide to the insurability of GDPR fines across Europe that includes common issues faced by organisations in international cyber scenarios and is illustrated with practical case studies.