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

DLA Piper GDPR fines and data breach survey: January 2022

DLA PIPER

DLA Piper GDPR fines and data breach survey: January 2022

This is the fourth annual DLA Piper fines and data breach survey since the application of the EU General Data Protection Regulation ("GDPR") on 25 May 2018.

It has been another busy period for enforcement with new record-breaking fines taking the top two spots on the GDPR fines league table and several notable court and supervisory authority decisions. Organisations and privacy professionals have also been kept busy this year dealing with the fallout of the decision by the Court of Justice of the European Union ("CJEU") in the case known as *Schrems II*.[1] The judgment has profound implications for transfers of personal data from Europe to "third countries". Recent case-law in France potentially expands this challenge to cloud services hosted entirely within Europe where they are provided by vendors subject to third country interception laws. Data localisation may not be sufficient to address *Schrems II*.

With thanks to the many different contributors and supervisory authorities who make this report possible,[2] our fourth annual survey takes a look at key GDPR metrics across the European Economic Area ("EEA") and the UK[3] since GDPR first applied and for the year commencing 28 January 2021. The EEA includes all 27 Member States of the EU plus Norway, Iceland and Liechtenstein.

"There has been a sevenfold increase in GDPR fines this year with just under EUR1.1bn (USD1.2bn/ GBP0.9bn)[4] fines imposed since 28 January 2021 compared to EUR158.5m (USD179m/GBP132m) during the same period last year.[5] Fines may be grabbing the headlines but the Schrems II judgment and its profound implications for data transfers continues to be a major challenge for organisations caught by GDPR."

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

2 This survey 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.

3 The UK left the EU on 31 January 2020. The UK has implemented GDPR into law in each of the jurisdictions within the UK (England, Northern Ireland, Scotland and Wales). As at the date of this survey the UK GDPR is the same in all material respects as the EU GDPR. That said, the UK Government Department for Digital, Media, Culture and Sport recently consulted on proposed changes to UK data protection laws *"Data: a new direction"* and is proposing to legislate changes to UK data protection laws during the course of 2022. It remains to be seen the extent to which these changes will deviate from the EU GDPR.

4 In this report we have used the following exchange rates: EUR 1 = USD 1.13/GBP 0.83.

5 This survey only covers GDPR fines so does not include fines imposed under other regimes, such as the two large fines recently imposed by the CNIL on Meta and Google for EUR60m and EUR150m respectively for infringements of the e-Privacy Directive as implemented under French law.

Summary and key findings

Record-breaking new fines

This year has seen two record breaking GDPR fines.[6] The first was imposed by the Luxembourg data protection supervisory authority against a US based online retailer and e-commerce platform for EUR746m (USD843m/GBP619m). The second was imposed by the Irish Data Protection Commission on WhatsApp Ireland Limited for EUR225m (USD254/GBP187m). Both fines are subject to ongoing appeals.[7]

Sevenfold increase in value of aggregate fines imposed

This year supervisory authorities across Europe have issued[8] a total of EUR1.087bn (USD1.23bn/GBP0.9bn) in fines since 28 January 2021, which is a sevenfold increase on the total of EUR158.5m (USD179m/GBP132m) issued in the year from 28 January 2020. Much of this increase is due to the two record-breaking fines referenced above. Fines may be grabbing the headlines but the *Schrems II* judgment and its profound implications for data transfers continues to be a major challenge for organisations caught by GDPR.

Country aggregate fines league table

It's all change at the top of this year's country league table for the aggregate fines imposed to date with Luxembourg and Ireland replacing Italy and Germany in the top two spots and Italy moving down to third place with EUR746m (USD843m/GBP619m), EUR226m (USD255m/GBP188m) and EUR79m (USD89m/GBP66m) respectively.

Significant increase of breach notifications

The trend of increasing numbers of data breach notifications has also continued over the last year. For the year commencing 28 January 2021, there have been more than 130,000 personal data breaches notified to regulators and on average 356 breach notifications per day, an 8% increase on last year's daily average of 331 notifications.[9]

Successful appeals

This year has also seen some successful appeals against decisions and penalties imposed by data protection supervisory authorities. Notably, the German data protection supervisory authorities are continuing to find difficulties in making fines stick. The headline EUR14.5m (USD16.4m/GBP12m) fine imposed by the Berlin data protection supervisory authority against Deutsche Wohnen SE for alleged infringements of the storage limitation principle was held to be invalid by the Regional Court of Berlin on the basis that the Berlin DPA failed to specify acts of the management of Deutsche Wohnen SE which were in breach of GDPR and therefore did not satisfy the requirements of the German Act on Regulatory Offences.[10] The public prosecutor in consultation with the Berlin DPA has now appealed the Regional Court's decision. This follows a decision by the Bonn Regional Court in November 2020 reducing a EUR9.6m (USD10.8m/GBP8m) fine against 1&1 Telecom on the basis the original fine was "unreasonably high". As noted in last year's survey following the 90% and 80% reductions of the fines originally proposed by the UK ICO for two data breaches, given there is so much legal uncertainty and so many open legal questions concerning GDPR, it often pays to appeal and to mount robust challenges to proposed regulatory sanctions.

6 All references in this survey to infringements or breaches of GDPR and to fines imposed are to findings made by relevant data protection supervisory authorities. In a number of cases, the entity subject to the fine has disputed these findings and the findings and penalties imposed are subject to ongoing appeal procedures. DLA Piper makes no representation as to the validity or accuracy of the findings made by relevant supervisory authorities.

7 WhatsApp has applied to the Court of Justice of the European Union to annul the decision of the European Data Protection Board. A summary of the grounds of appeal is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021TN0709&from=EN.

8 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.

9 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, including Germany, which has previously had high numbers of data breach notifications. 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.

10 There is ongoing debate in Germany whether the German Act on Regulatory Offences, which requires proof of specific acts of infringement by the management of legal persons, is consistent with GDPR, which includes no such requirement when imposing fines.

Highest individual fine league table

#1

Luxembourg – EUR746m

Luxembourg's data protection supervisory authority, the CNPD, takes pole position this year with a fine of EUR746m (USD843m/ GBP619m) against a US online retailer and e-commerce platform. The fine is not publicly available and is subject to an ongoing appeal.

#2

Ireland – EUR225m

On 2 September 2021 the Irish Data Protection Commission ("DPC") issued a fine of EUR225m (USD254m/GBP187m) against WhatsApp Ireland Limited for various findings of failings to comply with the GDPR transparency requirements as well as a reprimand and order to bring its processing into compliance. WhatsApp has appealed to the CJEU to annul the decision (Articles 5(1)(a), 12, 13 and 14 GDPR).

#3

France – EUR50m

The Luxembourg and Irish fines have moved last year's top fine issued by France's data protection supervisory authority, the CNIL, into third place. The CNIL fined Google EUR50m (USD56.5m/GBP41.5m) for various findings of failings to comply with transparency requirements and for failing to have an adequate legal basis for processing in relation to personalised advertising (Articles 5, 6, 13 and 14 GDPR).

Spotlight on enforcement of data transfer rules

The *Schrems II* judgment

The decision of Europe's highest court in *Schrems II* in July 2020 was seismic. The CJEU invalidated the Privacy Shield regime and left standard contractual clauses on life support – which are by far the most common mechanisms to legitimise transfers of personal data from Europe. It was also expressly stated that a controller established in the EU and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned. Since the judgment, both regulators and the regulated have been trying to find clarity as to what it actually means in practice for international transfers of personal data while privacy activists continue to stir the pot by issuing multiple follow-on complaints.

Regulatory guidance provides some clarity

On 18 June 2021 the European Data Protection Board finalised its recommendations on how organisations should comply with the judgment.[11] These are not legally binding but will be followed by supervisory authorities to inform enforcement decisions and will carry weight in the courts. Among other things, the recommendations require comprehensive mapping of data transfers and transfer impact assessments where individual transfers rely on standard contractual clauses or binding corporate rules. The EDPB acknowledges that mapping transfers "can be a complex exercise" particularly as organisations are required to consider the entire end to end supply chain including onward transfers. Where an organisation identifies a transfer that relies on standard contractual clauses or binding corporate rules, the recommendations require the exporter (where appropriate in collaboration with the importer) to assess whether any laws or practices in the third country to which the data are sent may impinge on the effectiveness of the transfer tool relied upon for that specific transfer.

Where problematic laws or practices are identified (which is almost always the case), the exporter is required to put in place effective supplementary measures to ensure an essentially equivalent level of protection of the personal data in the third country to the protections offered by European laws. There is an exception where the exporter determines that the problematic laws will not be applied in practice to that particular transfer, supported by a documented assessment.

New standard contractual clauses help to reduce the compliance gap

Also in June 2021 the European Commission helped to reduce the compliance gap to some extent by issuing updated standard contractual clauses which take into account the EDPB recommendations so far as they relate to contractual supplementary measures.[12] However, these new clauses still require organisations to complete transfer impact assessments and may not be sufficient to achieve equivalent protection without additional organisational and technical measures.

Meeting the requirements of *Schrems II* and the EDPB recommendations is a very significant undertaking requiring a complicated assessment of the laws and practices of typically multiple third countries to which personal data are transferred or can be accessed from.[13] It is a challenge even for the most sophisticated and well-resourced organisations and is beyond the means of many small and medium-sized enterprises.

11 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0 Adopted 18 June 2021.

12 Commission Implementing Decision (EU) 2021/914 of 4 June 2021. The new standard contractual clauses do not apply in the UK. The UK ICO recently completed a consultation on proposed new UK standard contractual clauses and we expect these to be finalised during 2022.

13 The DLA Piper Transfer toolkit and methodology has been deployed by more than 100 organisations to assess exports of personal data from the UK and EEA to third countries in light of the *Schrems II* judgment and EDPB recommendations. We now have more than 45 comparative assessments of third country laws and practices in our library and available with the toolkit. Please get in touch with your usual DLA Piper contact or email dataprivacy@dlapiper.com for more details.

"Meeting the requirements of Schrems II and the EDPB recommendations is a challenge even for the most sophisticated and well-resourced organisations and is beyond the means of many small and medium-sized enterprises."

Continuing legal uncertainty

While the EDPB recommendations bring a degree of clarity, many important open legal questions remain regarding Chapter V GDPR and the application of the *Schrems II* judgment. A key question is whether the concept of proportionality enshrined in EU law and explicitly included in Article 24 GDPR can be applied to reduce the compliance burden created by *Schrems II*. The heart of the problem is a conflict of international laws between third country laws permitting interception of personal data by public authorities on the one hand and the protections required by European data protection laws on the other. In the long-term this can only be fixed by an international agreement driving changes to the underlying problematic domestic laws and practices to ensure equivalent rights and protections to those afforded under GDPR.

Evolving enforcement landscape

It also remains to be seen how actively data protection supervisory authorities will enforce these requirements in practice.

As at the date of this survey there have been no publicly reported GDPR fines imposed for infringements of the international transfer restrictions. However, this is certainly not the full story, with notable developments both among supervisory authorities and in the courts.

NOYB complaints

One month after the *Schrems II* judgment, Maximillian Schrems through his organisation "My Privacy is None of Your Business" (NOYB) filed 101 complaints against a wide range of data exporters across Europe for their alleged continued transfer of personal data to Facebook and Google in the US in breach of the *Schrems II* and GDPR Chapter V requirements.[14] The EDPB responded by creating a taskforce to ensure consistency across Member States when responding to complaints relating to international transfer restrictions. Following a complaint filed by NOYB against the European Parliament, the European Data Protection Supervisor ("EDPS") recently issued a formal reprimand to the European Parliament for breach of (among other violations) Article 46 and Article 48(2)(b) GDPR. The EDPS held that the European Parliament had failed to ensure an essentially equivalent level of protection was provided to personal data transferred to the US in the context of the use of cookies on a European Parliament website, in accordance with *Schrems II*. This is the first decision to be issued as a result of the NOYB complaints and provides some insight into the likely approach by data protection regulators in relation to the other complaints filed and more generally in relation to enforcement of international transfer restrictions.[15]

14 Details of the 101 complaints are available at www.noyb.eu.

15 A copy of the EDPS decision is available at: https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf.

Ongoing Member State investigations

Several Member State supervisory authorities have opened ongoing investigations into how exporters are complying with international data transfer restrictions, notably in Belgium[16], Germany[17], Greece[18] and Ireland.[19]

In June 2021, various state data protection authorities in Germany launched a coordinated investigation writing to selected companies using a joint questionnaire. Amongst other things the investigation is focussing on service providers used to send emails, host websites, provide web tracking analytics, manage applicant data and exchange customer and employee data within a group of companies.[20]

EDPS investigations

Two more notable investigations into data transfers were launched by the European Data Protection Supervisor ("EDPS") in May 2021.[21] The EDPS is the supervisory authority with responsibility for oversight of EU institutions and bodies and as such its decisions and rulings carry significant weight and influence with other supervisory authorities. One investigation concerns use of cloud services by EU institutions, bodies and agencies provided by Amazon Web Services and Microsoft. The other relates to the European Commission's use of Microsoft Office 365. The investigations are ongoing.

Cases and enforcement activity

There have also been some notable cases and regulatory enforcement activity this year considering the application of the *Schrems II* and Chapter V GDPR requirements to specific transfers. These include:

- In March 2021 France's highest administrative court considered the application of the *Schrems II* decision to data hosted with an EU-based processor which was a subsidiary of a US company.[22] The Conseil d'Etat concluded that a platform processing personal data used to book COVID-19 vaccinations had sufficient legal and technical safeguards in place to protect personal data from unauthorised access and therefore rejected a claim brought by various French professional associations and unions demanding the suspension of the service. The reason this ruling is noteworthy is that although the claimants were unsuccessful, the court concluded that *even where there is no transfer of personal data to a third country* where the EU-based service provider is a subsidiary of a company subject to US law, there was a risk that personal data could be accessed by US public authorities using extra-territorial US laws. The ruling also implies that merely localising and ring-fencing personal data in Europe may not be sufficient where the service provider is subject to extra-territorial laws that may result in access to personal data by public authorities in third countries; additional safeguards may be necessary to prevent access.

16 Investigations relate to the 'My Privacy is None of Your Business" 101 complaint.

17 See https://edpb.europa.eu/news/national-news/2021/coordinated-german-investigation-international-data-transfers_en for further information.

18 The Greek regulator, the HDPA, is currently investigating four complaints against data controllers established in Greece, concerning infringements of the provisions of Chapter V of the GDPR.

19 The Irish Data Protection Commission is currently investigating a number of companies in relation to international data transfer restrictions.

20 Details of the joint investigation and the questionnaires sent are available at https://datenschutz-hamburg.de/pages/fragebogenaktion/.

21 The EDPS press release announcing the two investigations is available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en.

22 The Conseil d'Etat press release (in English) and full decision (in French) are available at https://www.conseil-etat.fr/Pages-internationales/english/news/the-urgent-applications-judge-does-not-suspend-the-partnership-between-the-ministry-of-health-and-doctolib-for-the-management-of-covid-19-vaccinati.

- Also in March 2021, the Bavarian data protection authority[23] in Germany issued a notice to a data exporter in relation to its use of the US-based email marketing service, Mailchimp, to send newsletters to customers which required the transfer of customer email addresses from the German data exporter to Mailchimp in the US.[24] The Bavarian DPA concluded that the data exporter had failed to carry out a transfer impact assessment to determine whether additional measures were necessary to make the transfer compliant, noting that Mailchimp may in principle be subject to surveillance by US intelligence services. The Bavarian DPA did not impose a fine on the controller, accepting that the use of the email marketing service was limited since it had only been used twice by the data exporter and noted that no special category personal data was involved. They also took note of the fact that – at the relevant time – the EDPB recommendations had not yet been finalised and that the data exporter agreed to immediately cease using the email marketing service.
- In April 2021, the Portuguese Data Protection Authority (CNPD) ordered the Portuguese National Institute for Statistics to suspend (within 12 hours) the sending of personal data from the Portuguese census in 2021 to the US and any other third countries without an adequate level of protection.[25] The decision followed a number of complaints and an investigation by the CNPD, which concluded that transferring census data to Cloudfare, Inc., a Californian undertaking which was directly subject to US surveillance laws, should be suspended, particularly in light of the highly sensitive nature of the personal data which related to almost all Portuguese citizens and included sensitive data such as health data and data relating to religious beliefs.
- In Ireland, the parties to the *Schrems II* saga continue to lock horns. The Data Protection Commission is examining Facebook Ireland Limited's compliance with Chapter V GDPR (in particular Article 46) in light of the judgment of the CJEU. Following the *Schrems II* judgment, the Data Protection Commission commenced a statutory inquiry into the lawfulness of Facebook's transfers of personal data relating to EU users to the US. The transfers in question were transfers between Facebook Ireland Ltd and Facebook's parent company. A Preliminary Draft Decision was delivered on 28 August 2020 which found that Facebook's transfers infringed the GDPR and included a preliminary order to Facebook Ireland Limited to suspend its data transfers to the US, a significant step towards enforcing the *Schrems II* ruling. Facebook initiated judicial review proceedings which sought to have this Preliminary Draft Decision set aside. The Irish High Court dismissed Facebook's challenge in May 2021, paving the way for the DPC's investigation to continue.

23 Specifically, the Bavarian data protection authority for the privacy sector – the *Bayerisches Landesamt für Datenschutzaufsicht*. Bavaria has two data protection authorities; one for the private sector and the other for public bodies.

24 For more information please refer to https://gdprhub.eu/index.php?title=BayLfD_(Bavaria)_-_LDA-1085.1-12159/20-IDV. An English summary of the decision is available at https://edpb.europa.eu/news/national-news/2021/bavarian-dpa-baylda-calls-german-company-cease-use-mailchimp-tool_en.

25 The decision is available at cnpd.pt. An English summary of the decision is available at https://edpb.europa.eu/news/national-news/2021/census-2021-portuguese-dpa-cnpd-suspended-data-flows-usa_en.

Data transfer predictions for 2022

For the coming year we predict:

- Data transfers are not going to stop anytime soon. We live in a hyper-connected world with many cloud vendors based in the US and other third countries. There will be a greater reliance in the coming year on the new Standard Contractual Clauses supplemented – where necessary – with additional contractual, organisational and technical measures. But the reality is that many transfers are likely to continue without these measures in place given the complexity and prevalence of international supply chains and for many organisations the unachievable compliance burden imposed by *Schrems II*.
- There will be a continued focus on data sovereignty and data localisation as a means to mitigate compliance exposure for international transfers of personal data and the rise of "fortress Europe", particularly in relation to higher risk transfers, for example those involving special category or criminal record data or personal data which is likely to be of particular interest to public authorities. Data localisation is not necessarily a complete solution where third country laws apply extra-territorially; additional safeguards may be required to prevent unauthorised access.
- There will be further enforcement activity by European data protection regulators. As the Bavarian DPA ruling demonstrates, the fact that big fines have not yet been issued does not mean that regulators have been idle. Regulators will typically write to exporters demanding they cease or regularise their transfers before moving to formal enforcement action. Much of the activity of regulators is unpublished. For many organisations it is the risk of having to agree to cease or significantly curtail transfers which is of greater concern than the theoretical risk of fines. Transfer suspension can be highly disruptive and have serious implications for business continuity.
- There will be broadening enforcement activity by financial regulators. 2021 saw some enforcement activity by financial regulators concerned about systemic disruption to IT systems due to uncertainty around international data flows. More of this activity is to be expected in 2022 as the new rules bed in. Moreover, businesses can expect to face scrutiny around data transfer compliance in the context of audits, due diligence, procurement processes and other compliance verification exercises.
- We may also receive formal decisions in relation to the various investigations mentioned above. Given the significance of these investigations, the decisions will very likely inform wider enforcement practice.
- International data protection laws will continue to evolve, which will require organisations to regularly update the comparative legal assessments required by the *Schrems II* judgment and EDPB recommendations.[26]
- There will be ongoing data mapping, transfer impact assessments and contract repapering activities. Many organisations still have much to do to regularise their existing transfers and to be able to demonstrate they have done so to ensure compliance with the GDPR accountability principle.

26 DLA Piper offers a subscription model to users of the DLA Piper Transfer toolkit which includes regular updates of third country comparative assessments to keep up-to-date with changes in law and practice. Please get in touch with your usual DLA Piper contact or email dataprivacy@dlapiper.com for more details.

Commentary

The main enforcement event during 2021 is undoubtably the very significant increase in the aggregate value of fines issued across the countries surveyed, jumping from EUR 158.5m (USD179m/ GBP132m) last year to EUR1.087bn (USD1.23bn/ GBP0.9bn) for the year starting 28 January 2021. The two record-breaking fines have also disrupted the country rankings for the value of fines issued by country, with Luxembourg and Ireland jumping from the bottom to the top two places in the rankings. Notably both of the record-breaking fines are subject to ongoing appeals so it's possible they will be overturned or reduced.

GDPR fines: big splash versus little and often

We do not include details of the number of fines issued in our survey as the data available are not sufficiently robust.[27] However, it is clear that whereas some supervisory authorities have opted to issue a very small number of larger high-profile fines, including Ireland, Luxembourg and the UK, other supervisory authorities have opted to issue many more fines often for quite small amounts. Italy and Spain are examples of the latter approach. There is an open question over which approach is most effective at driving better compliance.

While large fines attract lots of media attention and can act as a powerful deterrent, they also consume significant resources to investigate, enforce and to defend any appeals, particularly when the defendant organisations are large and well-resourced multinationals. When appeals are successful or when provisional notices to fine are very significantly reduced following challenge by the defendant organisation, this can also undermine the credibility of the enforcement process and reduce the deterrent effect of fines.

The alternative approach of fining little and often is preferred by the Italian and Spanish supervisory authorities, who collectively have issued several hundred GDPR fines since its application in May 2018. Organisations are much more likely to be fined for GDPR infringements in Spain and Italy relative to other countries surveyed. Smaller fines typically do not generate the same media interest, though Spain and Italy have also imposed some significant headline-making fines.

Evolving enforcement trends

This year has seen a continuation of the enforcement trends we identified in last year's report. The GDPR transparency principle remains an enforcement priority for supervisory authorities across the countries surveyed. The WhatsApp fine was in large part imposed as a result of findings that WhatsApp had failed to comply with the transparency principle and related information requirements (Article 5(1)(a) and 12 to 14 GDPR). Supervisory authorities are continuing to set a high bar for compliance with this requirement and for the linked requirement to be able to demonstrate a lawful basis to process personal data.

Fines resulting from findings of infringements of GDPR's integrity and confidentiality principle and related requirements to notify personal data breaches promptly continue to be common across all countries surveyed. Following the increase in cyberattacks during the pandemic, there has been a notable uptick in fines following investigations and findings by supervisory authorities of inadequate security measures. The Polish Data Protection Authority – PUODO – has been particularly active over the last year in relation to GDPR's information security requirements. It has issued

27 Supervisory Authorities do not publish details of all fines imposed and when they do, do not always differentiate between fines imposed under GDPR and fines imposed under other legal regimes, such as that created by the e-Privacy Directive 2002/58/EC as implemented.

multiple fines and has emphasised the importance of appropriate (cyclical) testing, measurement and evaluation of the effectiveness of information security measures. The PUODO suffered a setback in October 2021 when a Polish court overruled its decision imposing a fine on ID Finance on the basis of findings that insufficient security measures were in place to prevent the illegal downloading of a client database by an 'authorised' third party. When allowing ID Finance's appeal, the Polish court concluded that the data leakage was actually caused by a data processor to which the data controller entrusted the processing. The court held that although as controller ID Finance was responsible for compliance with GDPR, it was not responsible for a personal data breach arising from reasons attributable to the processor. This is a welcome development and although of limited precedential value outside of Poland, it does at least support an argument that controllers are not liable for all acts and omissions of their processors on a strict liability basis.

Consistency and Cooperation under the spotlight

When the GDPR was first adopted, its cooperation and consistency mechanism (under Chapter VII GDPR), a cornerstone of the "one-stop-shop", was heralded as one of the major benefits for regulated organisations compared to the legacy regime under the Data Protection Directive. Instead of having to engage with multiple local data protection authorities, organisations established in the EU would be able to deal with only a single data protection authority with respect to their cross-border processing activities. Under Article 60 and 63 GDPR, data protection authorities may refer issues that implicate multiple Member States to the EDPB to adopt a binding decision in accordance with Article 65. In relation to the Irish DPC investigation of WhatsApp Ireland Limited, which began in 2018, the final fine of EUR225m (USD254m/GBP191m) represents a significant increase from the EUR30m to EUR50m (USD34m – USD56.5m/GBP25.5m – GBP42.5m) estimated fine initially proposed by the DPC. However, pursuant to the GDPR's cooperation and consistency mechanism and following objections from the other EU supervisory authorities concerned, in a lengthy report the EDPB directed the Irish DPC to reassess the amount of the fine. The consistency mechanism has on this occasion resulted in a 350% increase in the fine originally proposed by the Irish DPC. Forum shopping – seeking to establish in Member States which have historically been more hesitant than others to impose large fines – is likely to be challenging in light of the consistency mechanism, and the much heralded one-stop-shop evidently does not mean a soft touch to achieve consensus. The WhatsApp fine suggests that the hawks are in the majority. WhatsApp has appealed to the CJEU asking them to annul the decision of the EDPB.

Diminishing threat of privacy class actions?

Compliance risks arising under GDPR are not limited to regulatory fines, suspension orders and other regulatory enforcement action. There is also the risk of follow-on claims for compensation. Article 82 GDPR provides that any person who has suffered "material or non-material damage" as a result of an infringement of GDPR has the right to receive compensation from the controller or processor for the damage suffered. What amounts to non-material damage remains an unsettled question of law, though it is clear from early case law that there is no need to prove financial loss to claim compensation; mere distress is sufficient. Helpfully, in April 2021 the Austrian Supreme Court referred several key questions regarding compensation for non-material damage under Article 82(1) GDPR to the CJEU,[28] including whether a mere breach of provisions of the GDPR in and of itself is sufficient for the award of compensation and whether non-material damage requires some harm that goes beyond mere annoyance.

28 A copy of the referral to the CJEU (in German) is available at: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20210415_OGH0002_0060OB00035_21X0000_001.

To add to the risk of individual claims, in some of the countries surveyed (notably the Netherlands and the UK) it is possible under domestic court procedural rules to combine claims into group claims potentially very significantly increasing the damages payable by the defendant organisation, making rich pickings for claimant lawyers and their funders in those jurisdictions where litigation funding and contingent fees are permitted.

On 10 November 2021, the UK's highest court, the Supreme Court, rejected a representative claim (very similar to the US-style opt-out "class action") brought by Richard Lloyd against Google.[29] The claim was brought on behalf of more than 4 million iPhone users, allegedly affected by a Safari Workaround that Google had deployed on certain Apple devices. The Supreme Court held that a data subject will not have a right to compensation for any contravention by a controller unless it can prove that the contravention has caused damage (i.e. mental distress or financial loss) to the individual concerned. In addition the Supreme Court held that the "novel" representative action was doomed to fail as Mr Lloyd had failed to show that there was either (1) an unlawful use of personal data relating to each individual, or (2) that the individual had suffered damage as a result. In addition, the Court held that a representative action was untenable on the facts on this case as it failed to satisfy the "same interest test".

The decision is undoubtedly a welcome one for any business that handles personal data which is subject to the UK GDPR and the jurisdiction of the English courts. Had Mr Lloyd's claim succeeded, controllers would have been exposed to similar class-action claims for compensation for unlawful processing of personal data or indeed mere loss of control of personal data arising from potentially any infringement of GDPR. The judgment is not, however, the end of representative actions. The Supreme Court reiterated their purpose and procedural advantages. However, to be able to bring a representative action in the UK, claimants will have to establish that their claims all satisfy the "same interest test". That is likely to be costly and complicated for most data protection claims.

It is important to note that court procedural rules differ among jurisdictions in Europe and not all jurisdictions can expect a reduction in the risk of group claims, including representative actions similar to US "class action". For example, in the Netherlands, Dutch law provides for a framework to bring class actions and provides a basis for compensation of non-financial loss. As a result, there has been an increase in claims made to courts on a representative "class action" basis in the Netherlands.

Predictions for the year ahead

Our predictions for the coming year include:

- Data transfers will continue to be an enforcement priority for regulators and a compliance priority for regulated organisations. Please refer to our Data Transfer Predictions for 2022 above.
- There will be significantly more complaints, investigations and enforcement activity this year in relation to cookies and similar tracking technologies. As with transfers, privacy activists are also wading in on the topic of cookie compliance. The organisation My Privacy is None of Your Business has issued 500 complaints to organisations across a wide range of sectors for alleged breaches of cookie requirements, threatening formal complaints to supervisory authorities if they do not remediate cookie use.[28]
- There will be more investigations and enforcement regarding organisations in the ad-tech ecosystem. For example, in the UK the Information Commissioner's Office announced in January 2021 that it was resuming its investigation into the adtech sector following a pause to focus on its response to the COVID-19 pandemic.[30]

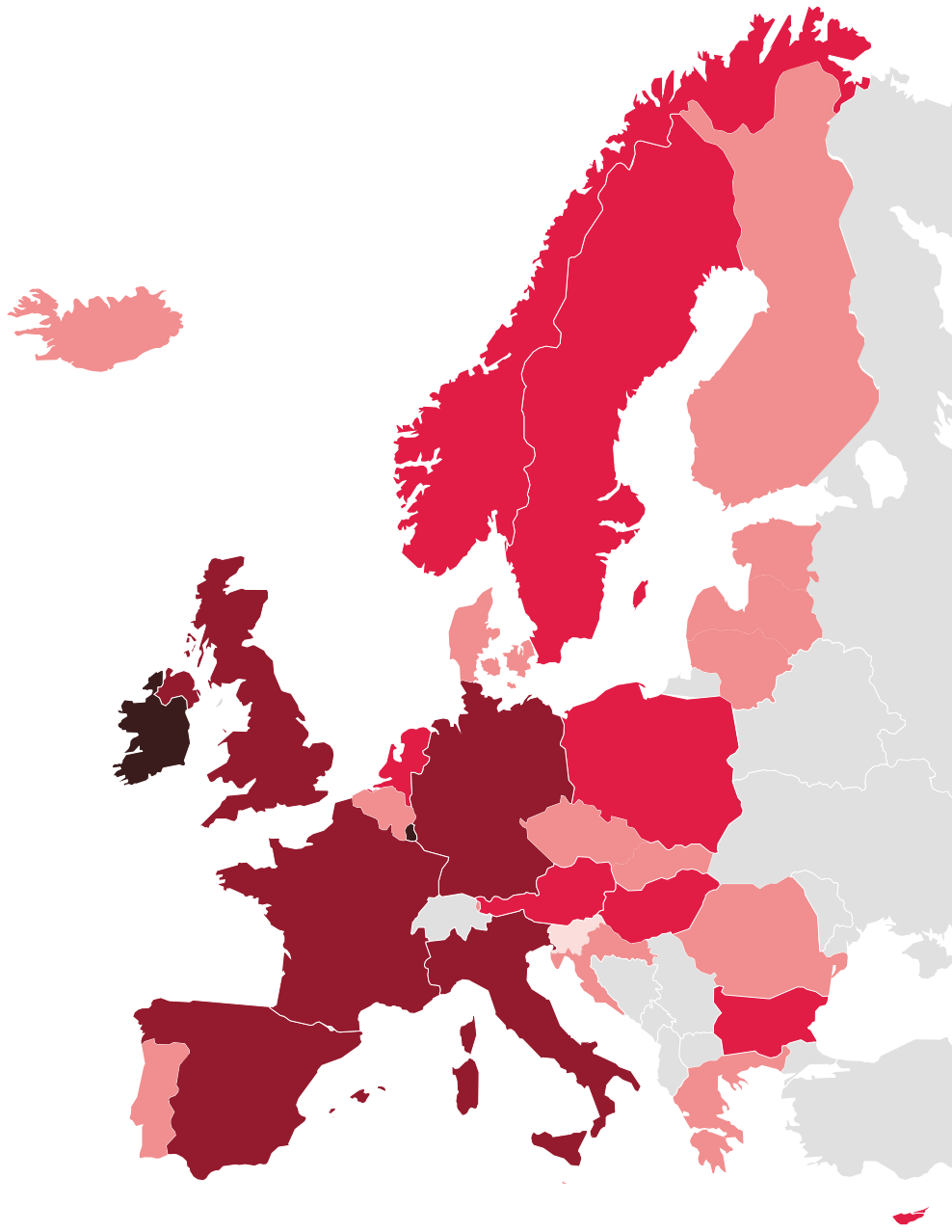
29 More information is available at https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints.

30 More information is available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/01/adtech-investigation-resumes/.

Report

Total value of GDPR fines imposed from 25 May 2018 to date (in euros)[31]

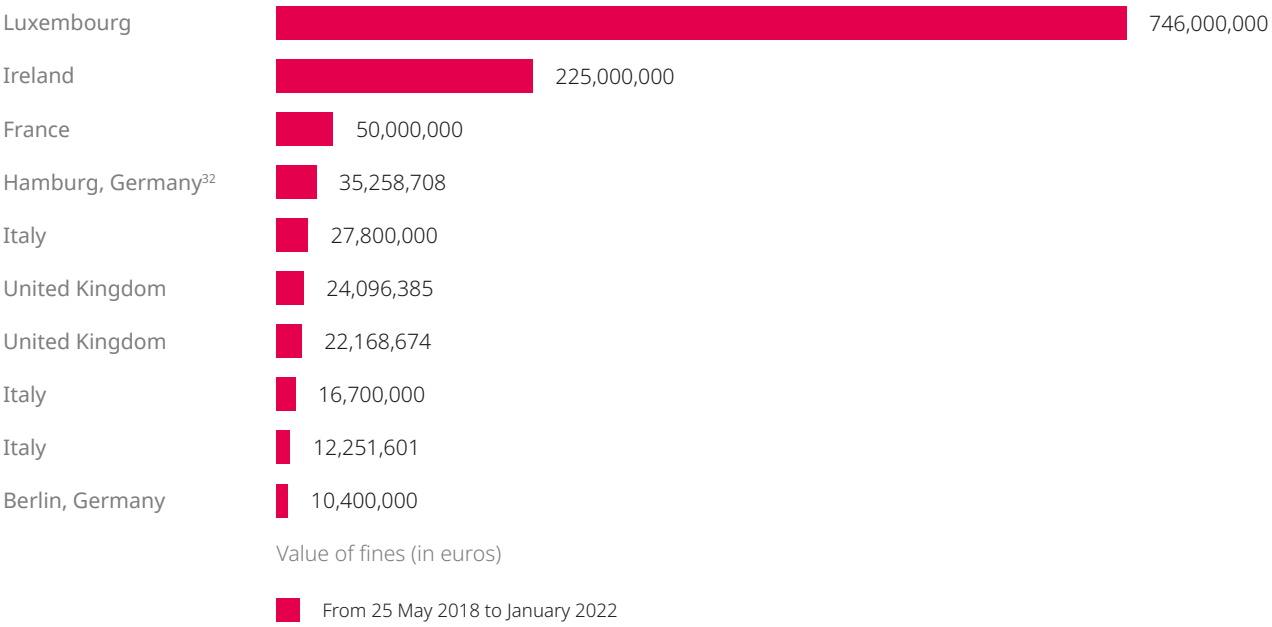
Luxembourg	746,299,400
Ireland	226,046,500
Italy	79,144,728
Germany*	69,329,916
Spain	61,024,128
France	58,580,300
UK	45,350,000
Austria	24,853,650
Sweden	18,000,000
Netherlands	8,964,500
Norway	7,834,034
Bulgaria	3,191,400
Poland	2,189,948
Hungary	1,312,100
Cyprus	1,244,600
Denmark	884,400
Greece	868,000
Finland	824,000
Romania	719,447
Belgium	508,000
Portugal	436,500
Czech Republic	416,515
Latvia	376,075
Slovakia	311,200
Lithuania*	244,500
Iceland	164,000
Malta	116,500
Croatia	88,000
Estonia	83,700
Liechtenstein	4,000
Slovenia	-



* Not all information in relation to fines by the different German DPAs is made publically available, therefore the real figure is likely to be higher than reported.
* In Lithuania, data in relation to minor fines imposed is not available and therefore the figure provided does not include the value of minor fines.

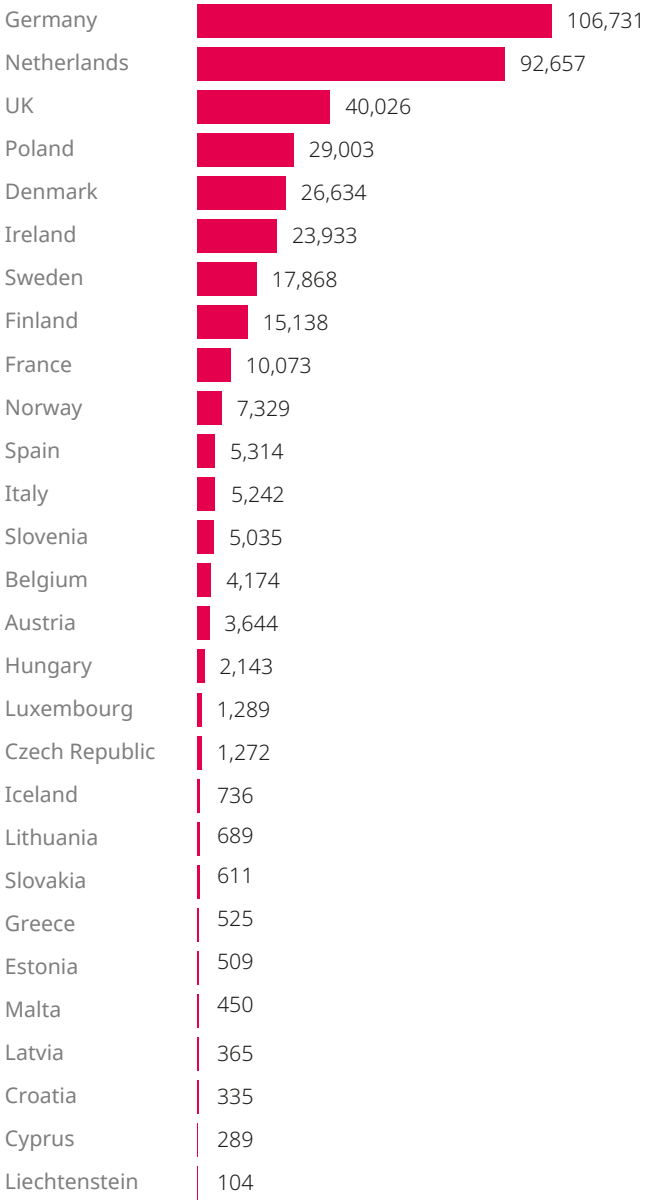
31 This report does not include fines that have been successfully appealed.

Top ten largest fines imposed to date under GDPR

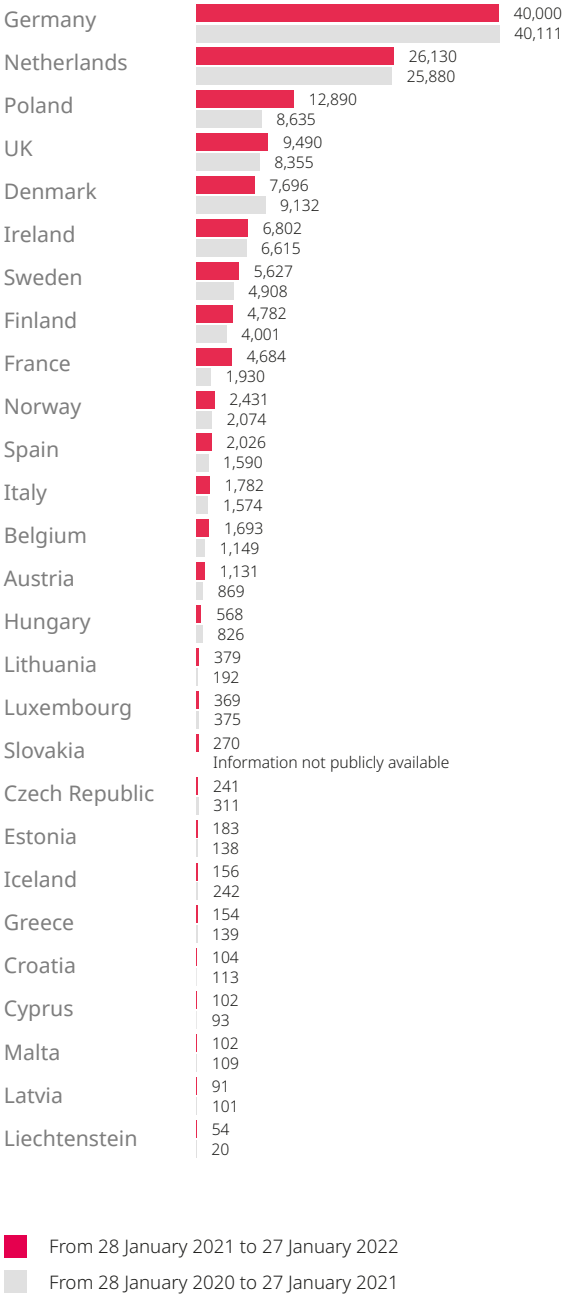


32 Germany has 16 different state data protection supervisory authorities, plus a federal supervisory authority.

Total number of personal data breach notifications between 25 May 2018 and 27 January 2022 inclusive*

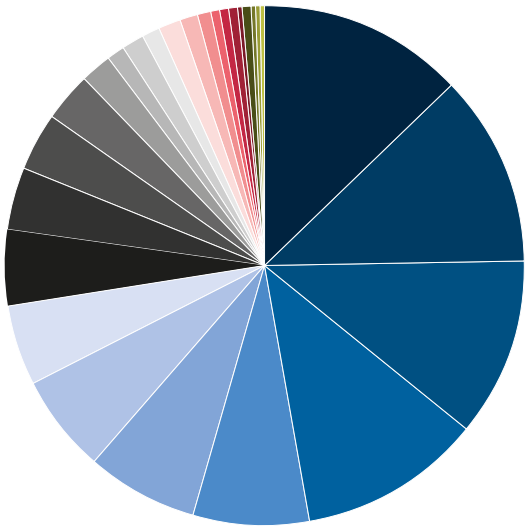


Total number of personal data breach notifications between 28 January 2021 and 27 January 2022 inclusive (last 12 month period)*



* 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. For the UK and Germany, no recent data is available regarding breaches notified during 2021 so we have had to extrapolate using the daily average rate for the previous year. 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 breach notifications per 100,000 population between 28 January 2021 and 27 January 2022 (last 12 month period)	Change compared to last year's ranking
Netherlands	**150.71**	+1
Liechtenstein	**136.02**	+6
Denmark	**130.60**	-2
Ireland	**130.19**	-1
Finland	**85.59**	No change
Germany*	**79.42**	+3
Slovenia	**71.70**	-3
Luxembourg	**57.76**	-1
Sweden	**54.83**	+1
Norway	**44.12**	+1
Iceland	**43.91**	-5
Poland	**33.75**	+1
Malta	**22.23**	-1
Estonia	**14.97**	+1
Belgium	**14.37**	+2
UK*	**14.14**	-2
Lithuania	**13.97**	+3
Hungary	**13.53**	No change
Austria	**9.60**	-3
Cyprus	**7.98**	-1
France	**6.88**	+3
Slovakia	**4.97**	Information not previously publically available
Latvia	**4.89**	-2
Spain	**4.28**	-2
Italy	**2.86**	+1
Croatia	**2.48**	-1
Czech Republic	**2.25**	-4
Greece	**1.45**	No change



* Per capita values were calculated by dividing the number of data breaches notified 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 2021 estimates).

* Breach notification statistics were not, at the time of publication, publicly available in the UK and Germany for 2021. We have, therefore, had to extrapolate the data to cover the relevant period.

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 provides an overview of key privacy and data protection laws across more than 100 different 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.

Transfer

In response to the *Schrems II* judgment, and taking into account subsequent recommendations of the European Data Protection Board, we have designed a standardised data transfer methodology ("Transfer") to assist organisations to identify and manage the privacy risks associated with the transfer of personal data regulated by the GDPR/UK GDPR to third countries. Transfer provides a basis by which data exporters and importers may logically assess the level of safeguards in place when transferring personal data to third countries. It follows a step-by-step approach comprising a proprietary scoring matrix and weighted assessment criteria to help manage effective and accountable decision-making. Transfer has already been deployed by more than 100 organisations to assess exports of personal data from the UK and EEA to third countries and we now have nearly 50 comparative assessments of third country laws and practices available. We offer a subscription model to users of Transfer, which includes regular updates of third country comparative assessments to keep up-to-date with changes in law and practice.

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 to create *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.