A REPORT BY DLA PIPER'S DATA, PRIVACY AND CYBERSECURITY TEAM

DLA Piper GDPR fines and data breach survey: January 2024

DLA PIPER

DLA Piper GDPR fines and data breach survey: January 2024

Ireland continues in pole position this year with the highest aggregate GDPR fines issued since 25 May 2018 and also takes the top spot for the largest ever fine imposed, relegating Luxembourg to second place. The total value of GDPR fines imposed in Ireland is now EUR2.86bn (USD3.12bn/GBP2.49bn).[1] The EUR1.20bn (USD1.31bn/GBP1.04bn) fine issued by the Irish Data Protection Commissioner in May 2023 against Meta Platforms Ireland Limited ("**Meta IE**")[2] is the highest ever issued.

As Ireland is a popular location for technology companies to set up their main establishment in the European Union ("**EU**"), it is not surprising that it has rocketed to the top spot of the country league table for the aggregate value of fines imposed.

Data driven social media and big tech remain the primary target for record fines across the countries surveyed with each of the top ten largest fines issued since 25 May 2018 being imposed on businesses in this sector. This year has seen the battle rage over the "grand bargain" which has enabled service providers to fund the development of progressive consumer services in exchange for monetising their data since the earliest days of the internet. It is now under sustained attack by European data protection supervisory authorities and Europe's highest court, the European Court of Justice ("**CJEU**").[3] Plans by some service providers to move to a "pay or okay" model are set for a bumpy ride with regulators and privacy activists. With so much at stake, the battle and debate over the future of the "free internet" is set to continue.

GDPR fines are not solely an issue for social media and big tech; European data protection supervisory authorities have grown in confidence year on year, with multiple fines issued during 2023 across a wide range of sectors. Notably Spain and Italy have opted for the little and often approach – issuing a large number of fines often for quite small amounts.[4]

1 In this survey we have used the following exchange rates: EUR1 = USD1.09/GBP0.87.

2 See: https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland.

3 See, for example: *Meta vs Bundeskartellamt* Case C-252/21 See: https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1652408.

4 We do not include details of the number of fines issued in our survey as the data available are not sufficiently robust. European data protection 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.

The GDPR restrictions on the transfer of personal data to third countries remain an enforcement priority for European data protection supervisory authorities, with the EUR1.20bn (USD1.31bn/GBP1.04bn) fine issued against Meta IE being the standout – but also multiple enforcement actions by regulators across the EU for alleged illegal transfers of personal data. Enforcement has not been limited to breach of transfer restrictions in 2023; GDPR core principles including security, transparency and the requirement for a legal basis to process continue to be enforcement priorities.

With thanks to the many different contributors and supervisory authorities who make this survey possible,[5] our sixth annual survey takes a look at key GDPR metrics across the European Economic Area ("**EEA**") and the UK.[6]

Ireland continues in pole position this year with the highest aggregate GDPR fines issued since 25 May 2018 and also takes the top spot for the largest ever fine imposed, relegating Luxembourg to second place. The total value of GDPR fines imposed in Ireland is now EUR2.86bn (USD3.12bn/ GBP2.49bn). The EUR1.20bn (USD1.31bn/GBP1.04bn) fine issued by the Irish Data Protection Commission in May 2023 against Meta Platforms Ireland Limited is the highest ever issued.

5 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 and Sorainen for their contributions in relation to Liechtenstein, Croatia, Bulgaria, Greece, Iceland, Malta, Cyprus, Estonia, Latvia and Lithuania respectively.

6 The survey takes a look at key GDPR metrics EEA and the UK since GDPR first applied on 25 May 2018 and for the year commencing 28 January 2023. The EEA includes all 27 Member States of the European Union plus Norway, Iceland and Liechtenstein. 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 is proposing to legislate changes to UK data protection laws and has published the Data Protection and Digital Information Bill. It remains to be seen the extent to which these changes will deviate from the EU GDPR.

Summary and key findings

Record breaking fines continue

This year has continued to see increasingly high GDPR fines, with yet another record breaking fine of EUR1.20bn (USD1.31bn/GBP1.04bn) issued by the Irish Data Protection Commission in May 2023, knocking the fine of EUR746m (USD813m/GBP649m) imposed by the Luxembourg data protection supervisory authority off the top spot.[7]

Rise in value of aggregate fines imposed

This year European data protection supervisory authorities have issued[8] a total of EUR1.78bn (USD1.94bn)/GBP1.55bn) in fines since 28 January 2023, which is an increase of 14.10% on the total of EUR1.56bn (USD1.70bn/GBP1.36bn) issued in the year from 28 January 2022. This is much smaller than the 50% increase reported last year, which has mainly been driven by a number of successful appeals in various jurisdictions, which have seen fines reduced or in some cases completely overturned.[9] During 2023 there were also fewer fines issued by European data protection authorities following opinions and binding decisions of the European Data Protection Board ("**EDPB**") under the GDPR consistency mechanism.[10] As reported in last year's survey, the EDPB has had a highly inflationary impact on the value of fines issued by European data protection supervisory authorities. This is in part due to timing – there have been a large number of referrals to, and consistency opinions issued by, the EDPB during 2023 but many of these have not (yet) crystalised into final fines being issued by the relevant supervisory authority.[11]

Country aggregate fines league table

There is no change at the top of this year's country league table for the aggregate fines imposed to date since 25 May 2018. Ireland and Luxembourg remain in the top two spots, with fines totalling EUR2.86bn (USD3.12bn/GBP2.49bn) and EUR746m (USD813m/GBP649m)[12] respectively. Given Ireland's popularity as a European headquarters for data driven social media and big tech businesses and the fact that the Irish Data Protection Commission is therefore frequently the lead supervisory authority for all cross-border processing throughout the EU, Ireland is likely to continue to be at the top of the table for years to come. As can be seen from the table of top ten GDPR fines issued to date, social media and big tech (which make up each of the top ten highest GDPR fines issued) continue to be the focus of European data protection supervisory authorities. The aggregate total fines reported since the application of GDPR on 25 May 2018 to 8 January 2024 now stands at EUR4.68bn (USD5.10bn/4.07GBP).

The GDPR's lead supervisory authority mechanism, coupled with the EDPB's role in the consistency and dispute resolution mechanisms, has led to the Irish Data Protection Commission playing a central role in shaping the interpretation of key aspects of GDPR, with key decisions during 2023 on issues such as transparency, data transfer and children's privacy. Importantly, many of these decisions are under appeal so businesses will continue to follow with interest as appeals work their way through the Irish and EU courts. Over five years following implementation of GDPR, legal certainty on some fundamental GDPR questions remains frustratingly out of reach.

7 All references in this survey to infringements or breaches of GDPR and to fines imposed are to findings made by relevant European 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.

8 Not all European data protection supervisory authorities publish details of fines. Some treat them as confidential. Our survey is, therefore, based on fines (and appeals) that have been publicly reported or disclosed by the relevant supervisory authority. It is possible that other fines (and appeals) have been issued on a confidential basis.

9 For example, the total value of GDPR fines issued in Denmark and Belgium have reduced from the previous figure reported in last year's survey.

10 Under Articles 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.

11 If European data protection supervisory authorities fail to respect an opinion issued by the EDPB, the EDPB may adopt a binding decision. See: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en?page=1.

12 This fine is subject to an on-going appeal which will be heard at a Luxembourg court in January 2024.

No change in the number of breach notifications made

Continuing the trend of the last couple of years, on average there were 335 breach notifications per day from 28 January 2023 to 27 January 2024 compared to 328 during the same period last year. Allowing for the margin of error, there is effectively no year-on-year change in the overall number of breach notifications made, although there are some notable changes within some jurisdictions.

The lack of overall change is, in part, due to a change in the way that some European data protection supervisory authorities have been reporting breach notification statistics with several supervisory authorities revising previously published breach notification statistics downwards.[13]

The levelling off is also consistent with the experience seen in other jurisdictions where breach notification laws have been introduced. It is a mandatory legal requirement under GDPR to notify personal data breaches to the competent supervisory authority unless the breach "*is unlikely to result in a risk to the rights and freedoms of natural persons*".[14] This threshold remains open to interpretation and with the consequences of notifying a breach now more apparent with multiple fines issued for data breaches coupled with follow-on litigation and compensation claims, organisations which may initially have erred on notification may now be shying away from doing so.

Germany,[15] the Netherlands, and Poland have reported the highest number of data breaches notified from 28 January 2023 to 27 January 2024, with 32,030, 20,235 and 14,167 respectively. Germany and the Netherlands also top the table for the total number of data breach notifications made between 25 May 2018 and 27 January 2024.

It is a mandatory legal requirement under GDPR to notify personal data breaches to the competent supervisory authority unless the breach "is unlikely to result in a risk to the rights and freedoms of natural persons". This threshold remains open to interpretation and with the consequences of notifying a breach now more apparent with multiple fines issued for data breaches coupled with follow-on litigation and compensation claims, organisations which may initially have erred on notification may now be shying away from doing so.

13 For example, in Slovenia, due to the fact that the GDPR-implementing law has now entered into force - there has been a change in the way notifications have been recorded. The figure of 6272 included in last year's survey for the total number of data breach notifications between 25 May 2018 and 27 January 2023, has been revised down to 675 (for the total number of data breach notifications between 25 May 2018 and 27 January 2024).

14 Article 33(1) GDPR.

15 Germany has 16 different state data protection supervisory authorities - not all information in relation to breach notifications has been made available by all of the supervisory authorities, and for some supervisory authorities, data is only available for part of the period of this survey and we have had to extrapolate the data. Therefore the real figure is likely to be higher than reported.

Highest individual fine league table

#1

In May 2023, the Irish Data Protection Commission imposed a record administrative fine of EUR1.20bn ((USD1.31bn/GBP1.04bn) against Meta IE,[16] as well as an order to suspend further transfers of personal data from the EEA to the US within five months, and an order to cease all unlawful processing of personal data transferred to the US in violation of GDPR. At issue in the inquiry underlying the Irish Data Protection Commission's decision was whether Meta's transfers of personal data from the EEA to the US, based on Standard Contractual Clauses ("**SCCs**") and supplementary measures as recommended by the EDPB, were legal following the *Schrems II* judgment.[17] In the decision, the Irish Data Protection Commission concluded that Meta IE's reliance on the updated 2021 SCCs did not compensate for the deficiencies in US law identified in *Schrems II*. Data exporters were able to breathe a sigh of relief on 10 July 2023 when the new EU to US adequacy decision was adopted by the European Commission based on the US Data Privacy Framework ("**DPF**") which was expedited following the Meta IE judgment. Under the new adequacy decision, EU based data exporters are permitted to export personal data to US based data importers which have signed up to the new DPF without having to rely on SCCs or any additional supplementary measures.[18] For the time being Meta will not have to cease transfers of personal data to the US. Less than 2 months after the new DPF and adequacy regime came into force, a French MEP submitted the first challenges to the European Union General Court demanding the immediate suspension of the adequacy decision and challenging the legality of the DPF itself.[19] It is far from certain whether the DPF will survive this challenge (as well as other anticipated challenges) so the sorry saga of data transfer enforcement and litigation and significant legal uncertainty for global businesses seems set to continue.

#2

Luxembourg's data protection supervisory authority, the CNPD, continues in the second position this year with a fine of EUR746m (USD813m/GBP649m) imposed against a US online retailer and e-commerce platform in 2021. The fine is not publicly available and is subject to an ongoing appeal.

#3

On 2 September 2022, the Irish Data Protection Commission imposed a record EUR405m (USD441m/GBP352m)[20] GDPR fine on Meta IE (in relation to Instagram). The Irish Data Protection Commission found that Meta IE, amongst other things, failed to comply with transparency requirements; lacked appropriate technical and organisational measures regarding the purpose of processing; failed to conduct a data protection impact assessment where processing was likely to result in a high risk to rights and freedoms of child users of Instagram, and failed to establish a legal basis for processing contact information data.

16 See: https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland.

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

18 See: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

19 See: https://www.politico.eu/wp-content/uploads/2023/09/07/4_6039685923346583457.pdf.

20 See: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry.

Spotlight on security of processing personal data

Fines resulting from breaches of Article 5(1)(f) – the integrity and confidentiality principle – and the related Article 32 – security of processing – continue to feature across all jurisdictions surveyed. For example, in September 2023, the Irish Data Protection Commission announced a fine of EUR345m (USD376m/GBP300m) against a social media provider for non-compliance with GDPR rules regarding the processing of personal data of child users. Among other infringements, the Irish Data Protection Commission concluded that the organisation had infringed the integrity and confidentiality principle (Article 5(1)(f) GDPR) by setting up its "family pairing" option in a manner that allowed non-child users, who could not be verified as being the parent or guardian, to implement less privacy protective settings in the child user's account.

What constitutes appropriate security measures meeting the standard required by Articles 5(1)(f) and Article 32 GDPR is likely to continue to be a key battle ground between regulators and the regulated in the years ahead. All the more so as a finding by a European supervisory authority that the legal standard of care for security and confidentiality has not been met makes it much easier for claimants to prove breach of law when bringing compensation claims or claims for breach of contract. While many decisions from European data protection supervisory authorities relating to the specific technical and organisational measures required to meet these GDPR requirements are the subject of ongoing appeals and debate, there is a growing body of fines and enforcement decisions which provide a helpful view of where supervisory authorities consider the legal standard of care is currently set.[21]

A failure to have appropriate governance and oversight over information security is one of the most cited aggravating factors by European data protection supervisory authorities when justifying penalties for security failures. A lack of appropriate or proper staff training and culture is also frequently referenced when justifying fines, along with a lack of risk assessments to properly understand and mitigate against information security threats that could impact personal data. The frequency and commonality of these findings is a clear signal that regulators expect information security to be effectively governed and managed across organisations from top to bottom. Senior leadership teams are expected to be across information security risks and, applying the GDPR's accountability principle, be able to demonstrate the efficacy of information security controls with appropriate reports and documentation.[22]

21 The legal standard for information security under Article 32(1) GDPR is set by reference to the "state of the art". As this is constantly evolving, what constitutes appropriate security today may not meet the legal standard of care in the future.

22 DLA Piper's Data, Privacy and Cybersecurity team has been tracking financial penalties under the GDPR and similar laws across selected jurisdictions and has built a new product called the DLA Piper TOMs Tracker. Please contact your usual DLA Piper contact for more information.

Spotlight on transfers

Transfers of personal data to third countries outside of the EEA are still grabbing the headlines, with the highest fine to date of EUR1.20bn (USD1.31bn/GBP1.04bn) issued by the Irish Data Protection Commission[23] for breach of Article 46(1) GDPR. Meta IE has commenced both an appeal and judicial review of the decision through the Irish courts as well as an appeal against the EDPB's decision in the case through the EU courts.[24]

At issue in the inquiry underlying the Irish Data Protection Commission's decision was whether Meta IE's transfers of EEA personal data to the US, based on SCCs, were lawful following the *Schrems II* judgment by the CJEU nearly three years previously. That judgment invalidated the EU-US Privacy Shield Framework, but also cast uncertainty on the use of SCCs to transfer personal data to the US, given the concerns noted by the Court about the US government's ability to access private sector data. In the wake of the *Schrems II* judgment, Meta IE adopted the 2021 updated version of the SCCs issued by the European Commission in June 2021 and implemented supplementary measures as recommended by the EDPB in November 2020 and June 2021.

In July 2022, the Irish Data Protection Commission first circulated its draft decision for review and comment by other European data protection supervisory authorities (also known as Concerned Supervisory Authorities ("**CSAs**"). After several CSAs lodged objections to perceived inadequacies of the draft decision in relation to the corrective measures proposed, the Irish Data Protection Commission referred the objections to the EDPB for determination pursuant to the Article 65 GDPR dispute resolution mechanism. The EDPB issued a binding determination to resolve the CSAs' dispute over whether the Irish Data Protection Commission should fine Meta IE in addition to suspending its data transfers and order it to bring its processing into compliance with the GDPR. The final Irish Data Protection Commission decision, which reflected that binding determination by the EDPB, included:

1. an order, made pursuant to Article 58(2)(j) GDPR, requiring Meta IE to suspend any future transfer of personal data to the US within the period of five months from the date of notification of the Irish Data Protection Commission's decision to Meta IE;
2. an administrative fine in the amount of EUR1.20bn (USD1.31bn/GBP1.04bn); and
3. an order, made pursuant to Article 58(2)(d) GDPR, requiring Meta IE to bring its processing operations into compliance with Chapter V of the GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EU/EEA users transferred in violation of the GDPR, within five months following the date of notification of the Irish Data Protection Commission's decision to Meta IE.

Although the Irish Data Protection Commission decision is limited to the facts in the Meta IE matter and was issued prior to the EU-US adequacy decision being adopted (see below), the decision provides a decidedly unambiguous message to thousands of companies that the costs and complexities of delivering their products and services in certain markets will increase. In particular, in its decision, the Irish Data Protection Commission concluded that Meta IE's reliance on the updated 2021 SCCs did not compensate for the deficiencies in US law identified in *Schrems II*. In addition, the Irish Data Protection Commission concluded Meta IE did not have in place any supplemental measures which would compensate for the inadequate protection provided by US law. In particular, the supplementary measures identified in Meta IE's transfer impact assessment ("**TIA**") did not *"provide essentially equivalent protection to EU law against the wide discretion the US Government has to access Meta US users' personal data via Section 702 FISA (PRISM) requests"*. It follows that transfers to other third countries, which have similar laws to the US in relation to public authority access, would have to overcome the same hurdles. The decision (which reflects the EDPB's binding determination) offers

23 See: https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf.

24 See: https://about.fb.com/news/2023/05/our-response-to-the-decision-on-facebooks-eu-us-data-transfers/.

yet another indicator that European data protection supervisory authorities are setting the bar high when it comes to supplementary measures used to protect EEA personal data however remote the risk of access to such data by public authorities. The decision also offers an insight on the inflationary impact of the EDPB's consistency and dispute resolution procedures when it comes to GDPR fines – the Irish Data Protection Commission had originally preferred not to issue a fine against Meta IE adopting the view that the suspension of data transfers to the US was appropriate, proportionate and necessary to ensure compliance with the GDPR – before being overturned on this point by the EDPB.

EU-US ADEQUACY

On 10 July 2023, the European Commission adopted its latest adequacy decision, for EU to US transfers with this latest decision based on the new EU-US Data Privacy Framework.[25] The DPF replaces the Privacy Shield Framework ("**Privacy Shield**") which was invalidated by *Schrems II* in July 2020. The adequacy decision allows personal data to flow from the EEA to DPF-certified US companies without the need for additional data protection safeguards. In a manner comparable to its predecessors, Privacy Shield and the EU-US. Safe Harbor Framework ("**Safe Harbor**"), the DPF enables certified companies that make legally binding commitments to comply with the DPF Principles to receive personal data from the EEA without having to rely on EU-approved transfer mechanisms such as SCCs or Binding Corporate Rules ("**BCRs**") and without having to conduct TIAs. The European Commission has concluded that the US ensures an adequate level of protection, comparable to that of the EU, for personal data transferred from the EU to US companies under the new DPF.

The European Commission has stated that the DPF introduces "*significant improvements compared to the mechanism that existed under the Privacy Shield*". An essential element of the US legal framework on which the adequacy decision is based concerns the Executive Order 14086 on 'Enhancing Safeguards for United States Signals Intelligence Activities' (EO). Notwithstanding the European Commission's assertion that the binding safeguards implemented pursuant to the EO "*address all the concerns raised by the European Court of Justice*," the new adequacy decision and the DPF on which it is based have already been contested. Max Schrems' privacy organisation, My Privacy is None of Your Business (NOYB), which led the previous legal challenges to both Privacy Shield and Safe Harbor, has already announced that it will also challenge the DPF.[26] Characterizing it as "*largely a copy of the failed 'Privacy Shield*,'" NOYB claims that "*there is little change in US law or the approach taken by the EU*" and that "*[t]he fundamental problem with FISA 702 was not addressed by the US, as the US still takes the view that only US persons are worthy of constitutional rights*." Less than two months after the EU-US adequacy decision was adopted, a French MEP also submitted challenges to the European Union General Court demanding the immediate suspension of the adequacy decision and challenging the legality of the DPF.[27] As predicted in last year's survey, it is likely that the EU – US adequacy decision will end up before Europe's highest court before long. Given the previous invalidations of Privacy Shield and Safe Harbor by the CJEU, the long-term durability of the DPF remains uncertain.

25 See: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

26 See: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

27 See: https://www.politico.eu/wp-content/uploads/2023/09/07/4_6039685923346583457.pdf.

Commentary

Ireland has taken the honours this year, both for the largest fine ever issued and the aggregate value of all fines issued to date under GDPR. In many of those cases, the fine originally proposed by the Irish Data Protection Commission was much lower than the final fine imposed after reference was made by other impacted European data protection supervisory authorities to the hawkish EDPB. The EDPB has been responsible for supercharging many of the fines originally proposed and for propelling Ireland up the rankings.

Ireland is likely to remain a popular location for US social media and big tech firms to set up their EU establishment given the familiar common law, language and favourable inward investment environment. Whichever EU jurisdiction is selected as a main establishment and lead supervisory authority, where cross-border processing of personal data impacts other Member States, the GDPR consistency mechanism is likely to be triggered resulting in references to the EDPB and invariably an increase to the originally proposed fine. Helen Dixon, the current Commissioner for Data Protection in Ireland, has announced that she will be stepping down in February 2024 after 10 years at the helm of Ireland's Data Protection Commission, having overseen a fundamental transformation of the regulation of personal data with the introduction of GDPR and then been at the forefront of many high profile enforcement decisions breaking new legal ground. The Commissioner will be replaced by a panel of up to three Commissioners and while the makeup of the panel and its approach to enforcement remains to be seen, Ireland will still be subject to the GDPR consistency mechanism so the new incumbents will have limited room for manoeuvre. It is also notable that a new chair of the EDPB, Anu Talus, was appointed in May 2023,[28] and her impact on where the focus of the EDPB will land in the coming years will be closely watched.

Several of the top ten largest fines ever issued under GDPR are the subject of ongoing appeals including the largest fine ever issued (against Meta IE) and the second largest fine ever issued (against a well-known on-line retailer). Even if these appeals are successful it is likely that the Irish Data Protection Commission will remain at or near the top of the rankings for as long as Ireland remains the popular choice for an EU establishment among data driven social media and big tech businesses.

2023 did see some successful appeals against decisions and penalties imposed by European data protection supervisory authorities. On 23 May 2022, the UK Information Commissioner's Office ("**ICO**") fined Clearview AI GBP7.6m (USD9.7m/EUR8.8m) for breaches of the UK GDPR. In October 2023, Clearview AI successfully appealed the ICO's enforcement action before the UK's information rights tribunal, on jurisdictional grounds. The tribunal determined that the (UK) GDPR did not apply to the processing of personal data by the company.[29] The UK Information Commissioner's Office has announced that it is appealing this decision.[30] Similarly, in Spain, the Spanish Data Protection Agency's (AEPD) first multi-million euro fine was overturned in its entirety by the Spanish National Court.[31]

28 See: https://edpb.europa.eu/about-edpb/who-we-are/edpb-chairmanship_en#:~:text=The%20EDPB%20is%20led%20by,for%20a%20five%20year%20term.

29 See: https://www.bailii.org/uk/cases/UKFTT/GRC/2023/819.pdf.

30 See: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/11/information-commissioner-seeks-permission-to-appeal-clearview-ai-inc-ruling/#:~:text=In%20its%20judgment%20the%20Tribunal,using%20AI%2C%20to%20foreign%20subscribers).

31 The AEPD has appealed this decision to the Spanish Supreme Court. See: https://www.poderjudicial.es/search/AN/openDocument/7096ceac19f38ec3a0a8778d75e36f0d/20230228.

Enforcement trends

Failure to comply with the core GDPR principles continues to be the most frequently cited justification for fines across the jurisdictions surveyed and of all the principles set out in Article 5 GDPR, failures to comply with the lawfulness, fairness and transparency principle (Article 5(1)(a) GDPR) remain the top enforcement priority. For example, when issuing a fine of EUR345m (USD376m/GBP300m) in September 2023 against a social media provider, the Irish Data Protection Commission concluded that the organisation had failed to provide adequate information to child users, infringing the rules on transparency and provision of information in Articles 12 and 13 of the GDPR; and used dark patterns to nudge child users into selecting more privacy-intrusive settings, infringing the principle of fairness (Article 5(1)(a)).

Similarly, both supervisory authorities and courts are continuing to set a high bar for compliance with the requirement to demonstrate a lawful basis to process personal data (another element of Article 5(1)(a)). The "grand bargain" at the heart of the free internet has allowed social media and big tech to fund progressive consumer services by monetising data they collect on users of those services. However, this grand bargain is under attack and was the subject of the very largest fines reported in last year's survey.[32]

In 2023, similar issues going to the heart of the grand bargain were considered by Europe's highest court. On 4 July 2023, the CJEU delivered its judgment in *Meta vs Bundeskartellamt*.[33] In its decision, the CJEU imposed strict limitations on the use of the lawful bases of contractual necessity, legitimate interests and consent.

The CJEU concluded that the legal basis of 'contractual necessity' (Article 6(1)(b) GDPR) can only be relied upon where the processing is "*objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject*". The Court held that while providing personalised content online to its users may be useful, it "*does not appear to be necessary*", as Meta IE (Facebook) could provide an "*equivalent alternative*" service to users that does not require personalised online content. In the context of Facebook's processing of user's personal data for the purposes of targeted online advertising, the CJEU concluded that Facebook could only rely on the legitimate interests legal basis (Art 6(1)(f) GDPR) if the users had been informed of the legitimate interest, the processing was strictly necessary, and the balance of competing interests lay in favour of the processing. The Court found that none of those conditions were met and that the processing was beyond the reasonable expectations of the user, especially as the processing was so extensive. In addition, the CJEU held that a controller's dominant market position did not prevent a user being able to validly consent to the processing of their data, however, it "*may create a clear imbalance*" between the data subject and the controller. Users must therefore be able to refuse their consent to any processing not necessary for the performance of the contract, "*without being obliged to refrain entirely from using the service*".

In last year's survey we predicted that there would be more enforcement in relation to behavioural advertising and the "grand bargain". The CJEU judgment referred to above is just one of several examples of cases and new fines imposed during 2023 relating to these issues.

32 See: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry; https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry; https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry and https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland.

33 *Meta vs Bundeskartellamt* Case C-252/21 See: https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1652408.

Significantly, on 27 October 2023, the EDPB adopted an urgent binding decision instructing the Irish Data Protection Commission to take final measures regarding Meta IE and to impose a ban on the processing of personal data for behavioural advertising on the legal bases of contract and legitimate interest across the entire EEA.[34]

The urgent binding decision followed a request from the Norwegian Data Protection Authority to take final measures that would have effect across the entire EEA. As a result of the EDPB's decision, Meta has announced that it plans to rely on consent as the legal basis for its behavioural advertising activities in respect of users in the EEA – using a subscription model where users who do not consent to share their personal data and receive targeted adverts will be charged a monthly fee. This so-called "pay or okay" model has already been the subject of significant debate among European data protection supervisory authorities[35] and been the subject of complaints from privacy activists, including by NOYB.[36]

This leaves open the question whether "free" services in exchange for the right to monetise users' personal data remains a viable approach under GDPR. Was it really the intent of GDPR to destroy that grand bargain that has funded so many progressive technologies which have (in large part) benefited society? This debate is far from over and as we reported in last year's survey, with so much at stake we anticipate much more enforcement, appeals, litigation and advocacy to lawmakers.

Looking back at our predictions for 2023

In last year's report we predicted more enforcement in relation to online service providers relying on behavioural advertising to fund consumer services; a bumpy ride for the new EU – US adequacy decision; and increased investigations and enforcement into the more invasive and personal data rich AI systems and solutions. Each of these predictions has come to pass. What lies ahead for 2024?

The battle continues to rage over the "grand bargain", which has enabled service providers to fund the development of progressive consumer services in exchange for monetising their data since the earliest days of the internet... was it really the intent of GDPR to destroy that grand bargain?

34 See: https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en

35 For example, on 22 March 2023, the Conference of Independent German Federal and State Data Protection Supervisory Authorities ("**DSK**") passed a resolution regarding the evaluation of so called pure subscription models ("**Pur-Abo-Modelle**") on websites. See: https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf (in German).

36 See: https://noyb.eu/en/meta-facebook-instagram-move-pay-your-rights-approach.

PREDICTIONS FOR THE YEAR AHEAD

Our predictions for the year ahead include:

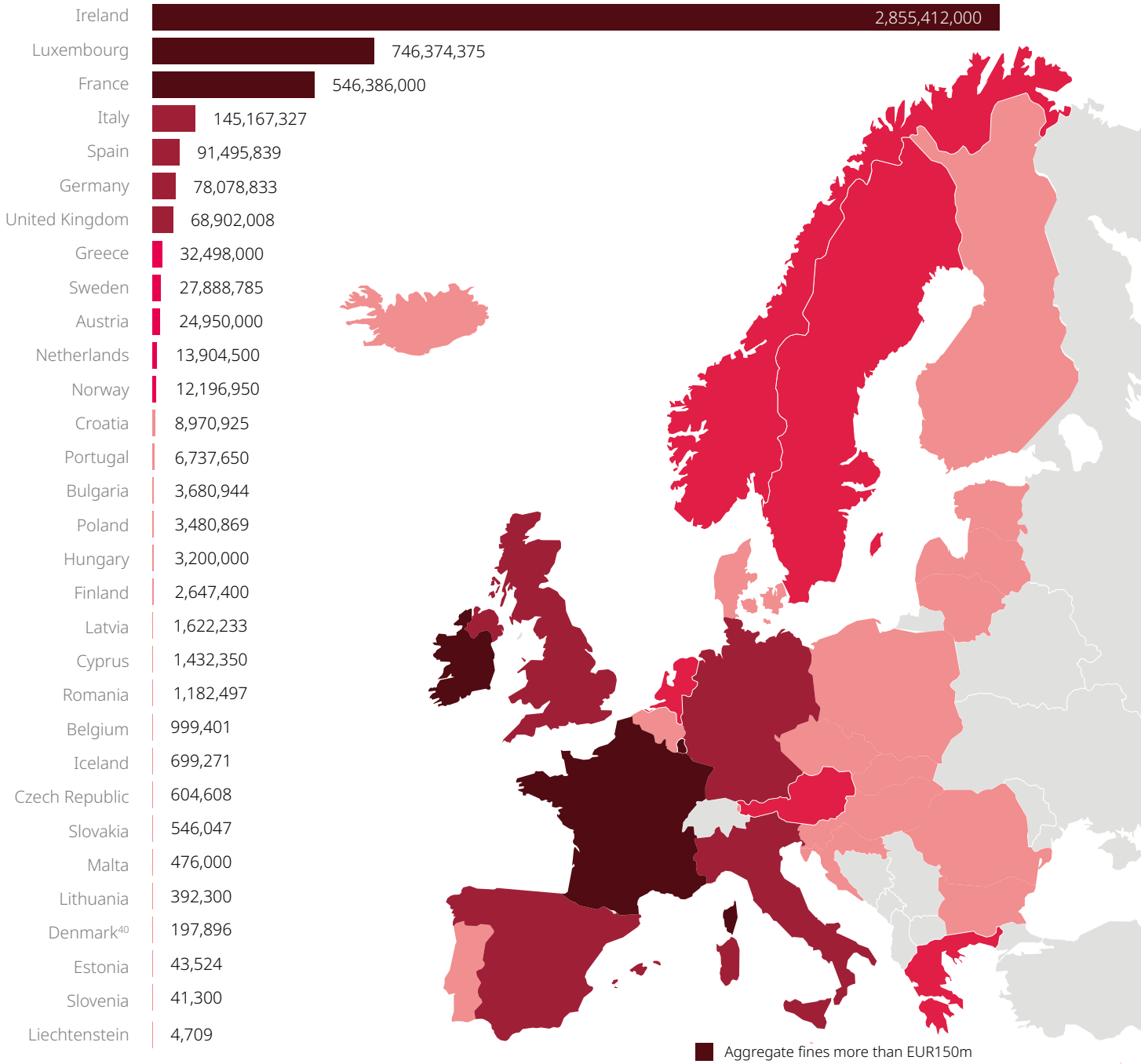
- There will be more regulatory enforcement, appeals and litigation relating to the "grand bargain" which has funded "free" progressive consumer services by monetising consumer data since the very earliest days of the internet and is now under sustained attack by European data protection supervisory authorities and Europe's highest court, the CJEU. We predict that the "pay or okay" model which some service providers are now proposing as an alternative will attract close regulatory scrutiny during 2024.
- There will be more bumps in the road for data transfers and the EU-US adequacy decision. With a French MEP already contesting the decision,[37] it seems almost inevitable that the EU – US adequacy decision based on the DPF will end up before Europe's highest court before long and it remains to be seen whether it will survive 2024 intact. As highlighted in last year's survey, transfers will continue to be a legal and compliance minefield for so long as the conflict of laws between GDPR and European Charter rights on the one hand and third country surveillance and interception laws on the other, remains.
- Given the long awaited e-Privacy Regulation, which was originally set to be published along with the GDPR back in 2018, is still no closer to approval, the EDPB has taken matters into its own hands and has recently published a consultation on draft guidelines on the scope of Article 5(3) of the e-Privacy Directive – i.e., the so-called 'cookie rule'.[38] The guidelines are broad in scope and conservative in their interpretation of the cookie rule, meaning that a wide variety of technologies other than traditional cookies are, in the opinion of the EDPB, caught by the rule. Given the current inconsistencies among organisations in obtaining consent for cookies, fuelled by the practical challenges of obtaining consent – we expect to see significantly more complaints, investigations and enforcement activity this year in relation to cookies and similar tracking technologies.
- With the explosion of new AI technologies continuing this year, we also predict continued investigations and enforcement into the more invasive and personal data rich AI systems and solutions. As AI continues to develop at pace, and new risk and opportunities continue to emerge, along with the raft of new guidelines and legislation in relation to AI – including the EU's AI Act – organisations and European data protection supervisory authorities alike will continue to grapple with artificial intelligence.
- European data protection supervisory authorities will continue to prioritise the importance of governance and oversight, with more enforcement where governance is found wanting. With the raft of new EU data and cyber legislation expected to come into force during 2024 and 2025, governance frameworks, including actionable steps to help govern data and cyber risks at all levels of an organisation and independent assurance that control frameworks are effective, will be increasingly important for organisations both to be able to comply with specific requirements for effective governance frameworks such as Article 24 GDPR and to satisfy the accountability principle in Article 5(2) GDPR.

37 See: https://www.politico.eu/wp-content/uploads/2023/09/07/4_6039685923346583457.pdf.

38 See: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en.

Report

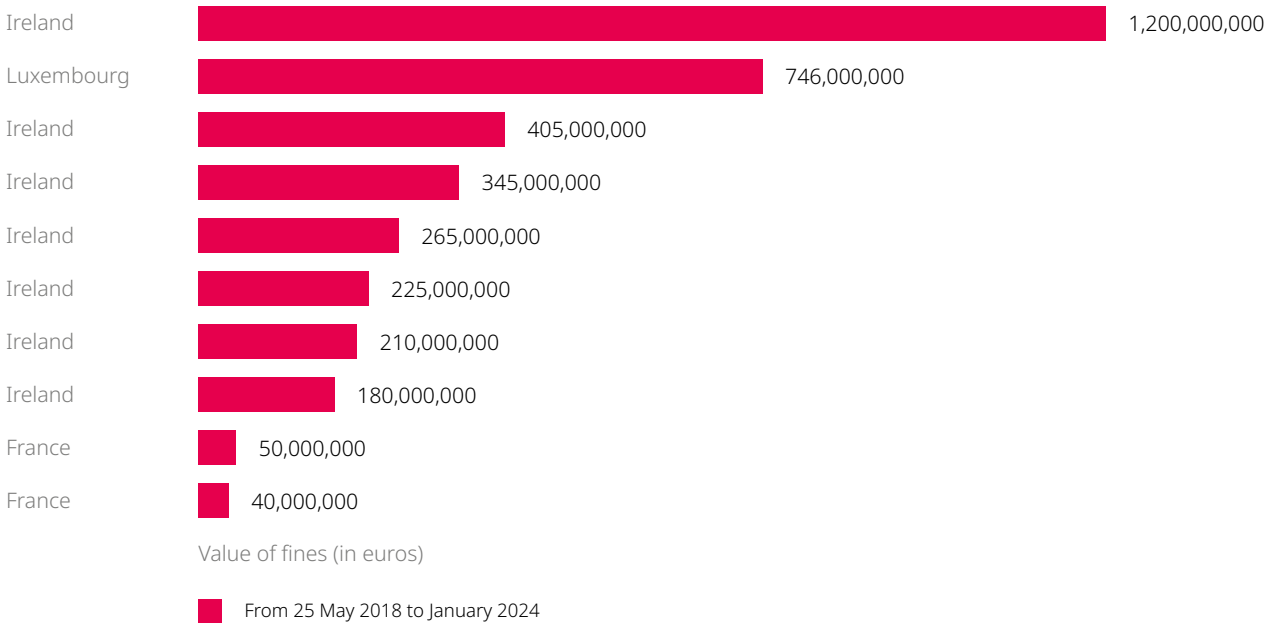
Total value of GDPR fines imposed from 25 May 2018 to date (in euros)[39]



39 This report does not include fines that have been successfully appealed. In some jurisdictions, not all information in relation to fines is made publically available (such as in relation to Germany) or only part of the data for the period of this report has been provided (e.g. Bulgaria). Therefore the real figure is likely to be higher than reported.

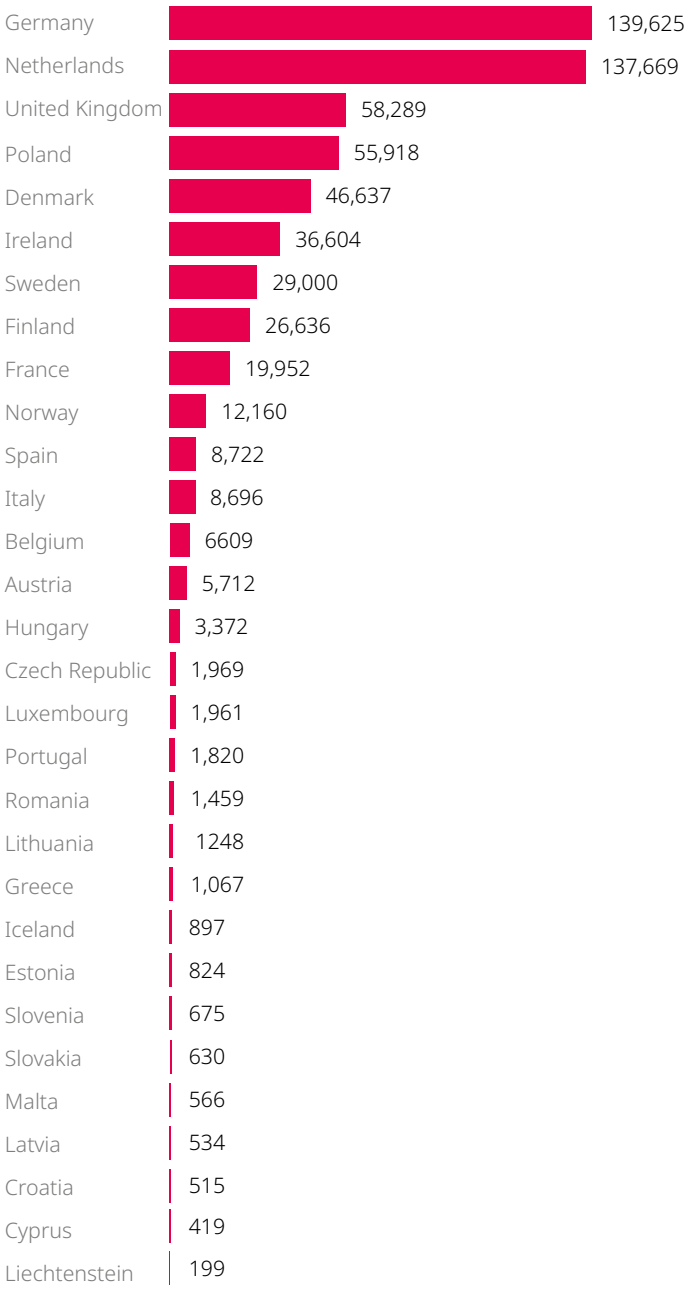
40 In Denmark, the supervisory authority ("**Datatilsynet**") does not have the authority to issue administrative fines. Instead, the Datatilsynet provides a recommendation as to the size of the fine and it is for the national courts to ultimately decide on the value of the fine imposed. In this survey, the total fine value reported reflects the actual fines imposed by the Danish courts, rather than the value of fines recommended by the Datatilsynet.

Top largest fines imposed to date under GDPR[41]



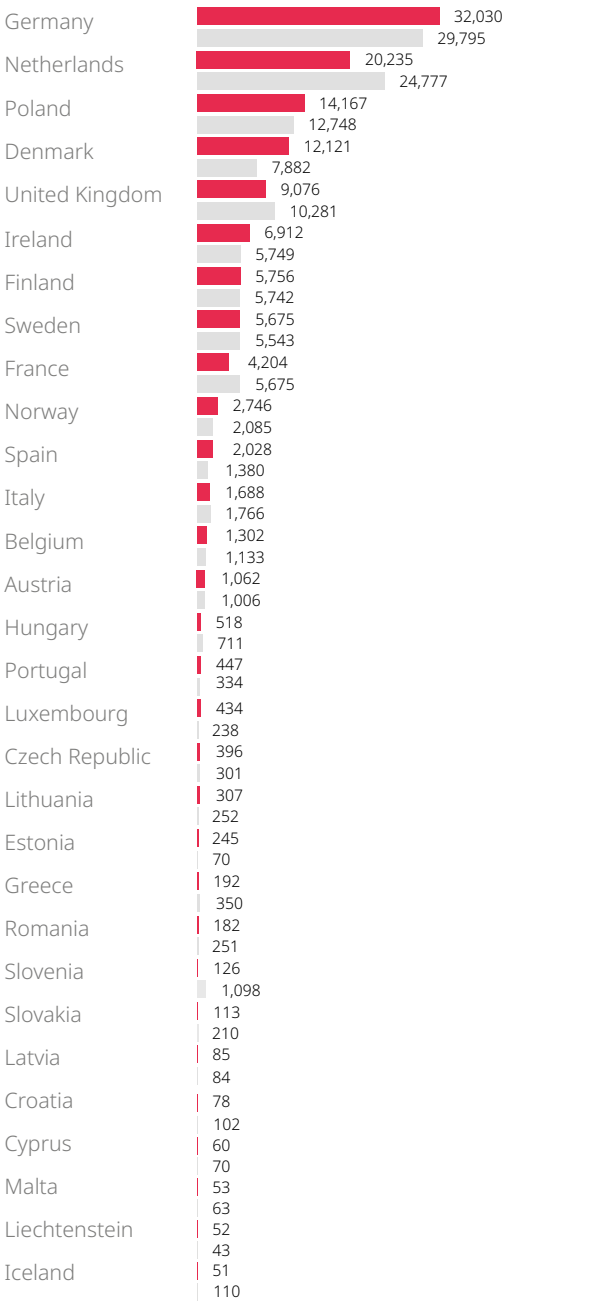
41 This report only includes fines imposed under the GDPR (so for example, it does not include fines imposed under other regimes such as e-privacy legislation).

Total number of personal data breach notifications between 25 May 2018 and 27 January 2024 inclusive



From 25 May 2018 to 27 January 2024

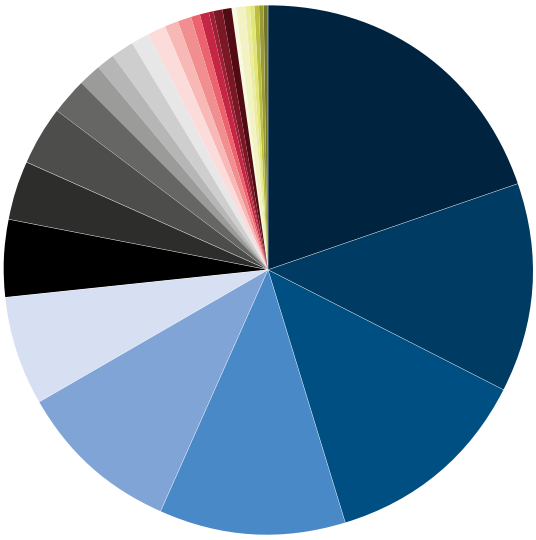
Total number of personal data breach notifications between 28 January 2023 and 27 January 2024 inclusive (last 12 month period)*



From 28 January 2023 to 27 January 2024
From 28 January 2022 to 27 January 2023

*Not all the countries covered by this report are included within this chart as they do not make breach notification statistics publicly available. In addition, many countries 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 using the daily average rate. Where we have extrapolated data in previous reports but have now been provided with more accurate data, we have updated the figures. It is also possible that some of the breaches reported relate to the regime before GDPR. In some jurisdictions there have been changes to the way that data breach notifications have been recorded which has impacted the rankings compared to last year. Some jurisdictions have not been included as no data is publicly available.

Per capita country ranking of breach notifications*	Number of breach notifications per 100,000 population between 28 January 2023 and 27 January 2024 (last 12 month period)	Change compared to last year's ranking*
Denmark	**203.82**	+1
Lichstenstein	**130.02**	+1
Ireland	**129.83**	+1
Netherlands	**115.87**	-3
Finland	**102.53**	No change
Luxembourg	**65.69**	+3
Norway	**49.05**	+1
Germany	**38.03**	+4
Poland	**37.29**	+1
Estonia	**20.41**	+10
Iceland	**14.06**	No change
United Kingdom	**13.32**	+1
Austria	**11.88**	+2
Lithuania	**11.56**	+3
Malta	**11.31**	-1
Belgium	**10.93**	No change
France	**6.13**	+1
Slovenia	**6**	-12
Hungary	**5.36**	No change
Sweden	**5.3**	-13
Latvia	**4.67**	+1
Cyprus	**4.57**	-1
Portugal	**4.37**	+1
Spain	**4.3**	+2
Czech Republic	**3.7**	+3
Italy	**2.77**	+1
Slovakia	**2.08**	-4
Croatia	**1.88**	+1
Greece	**1.83**	-4
Romania	**0.99**	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 2023 estimates).
* Full breach notification statistics were not, at the time of publication, publicly available for 2023 in a number of jurisdictions including Germany and the Netherlands (and others). We have, therefore, had to extrapolate the data to cover the relevant period. In addition, where data was previously not publicly available and extrapolated for 2022, this may have impacted upon last year's rankings. In some jurisdictions, such as Slovenia, there have been changes to the way that data breach notifications have been recorded which has significantly impacted their rankings. Not all data protection supervisory authorities have provided data breach notification data.

Additional resources

The DLA Piper data, privacy and cybersecurity 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 250 organisations to assess exports of personal data from the UK and EEA to third countries and we now have over 75 comparative assessments of third country laws and practices available. We offer an update service to users of Transfer, which includes regular updates to our tool and 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.