A REPORT BY DLA PIPER'S DATA, PRIVACY AND CYBERSECURITY TEAM
JANUARY 2025

DLA Piper GDPR fines and data breach survey

DLA PIPER

DLA Piper GDPR fines and data breach survey

It has been another busy period for enforcement with an aggregate total of EUR1.2bn (USD1.26bn/GBP996m)[1] of GDPR fines issued this year across all the countries surveyed. Ireland is still leading the category for the highest aggregate total of GDPR fines issued since 25 May 2018 - the Irish Data Protection Commission ("**Irish DPC**") has issued a total of EUR3.5bn (USD3.7bn/GBP2.91bn) since GDPR first applied. Ireland also remains in pole position for the largest fine ever imposed, with a fine of EUR1.2bn (USD1.26bn/GBP996m) issued against Meta Platforms Ireland Limited ("**Meta**") in 2023.[2]

Big tech companies and social media giants remain the primary targets for record fines across the countries surveyed, with nearly all of the top ten largest fines since 25 May 2018 being imposed on businesses in this sector. However, fines have not been restricted to tech companies and social media giants; European data protection supervisory authorities have demonstrated a growing confidence and assertiveness during 2024, issuing fines in other sectors, particularly focusing on breaches of the core GDPR principles, notably the lawfulness, fairness and transparency principle[3] and the integrity and confidentiality principle.[4] For example, there have been a number of fines issued against organisations within the financial services sector, including two fines totalling EUR6.2m (USD6.5m/GBP5.1m)[5] issued against a large bank by the Spanish Data Protection Authority ("**Spanish AEPD**") for a number of breaches of the GDPR, including inadequate security measures.

In Poland, the President of the Personal Data Protection Office ("**PUODO**") imposed administrative fines on several large international banks, including issuing a fine of EUR870,000 (USD913,500 /GBP722,100) for failing to notify customers of a data breach.[6] There have also been a number of fines issued against organisations in the energy sector. For example, in Italy, the Italian Data Protection Authority ("**Italian Garante**") issued a fine of EUR5m (USD5.25m/GBP4.15m) against a utility provider for using outdated or inaccurate customer data to execute unsolicited electricity and gas contracts. The company also failed to respond in a timely and comprehensive manner to requests to exercise data protection rights.[7]

As predicted in last year's report, European data protection supervisory authorities have continued to prioritise the importance of governance and oversight, with failings in governance and oversight being referenced as an aggravating factor in several enforcement decisions.

1 In this survey we have used the following exchange rates: EUR1 = USD1.05/GBP0.83. 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.

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

3 Article 5(1)(a) GDPR.

4 Article 5(1)(f) GDPR.

5 See: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2024-7797 and https://www.boe.es/diario_boe/txt.php?id=BOE-A-2024-18720

6 See: https://uodo.gov.pl/pl/138/3343

7 See: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10053275#1

In a notable example, the Dutch Data Protection Authority ("**Dutch DPA**") has announced that it is investigating whether it can hold the directors of Clearview AI personally liable for multiple violations of GDPR.[8] With organisations now grappling with the new laws and regulations forming part of the EU Digital Decade[9] and with several of these laws mandating greater governance and oversight and establishing the principle of personal liability for members of management bodies, this trend is set to continue.

With the rapid adoption of artificial intelligence enabled solutions and functionality, particularly by big tech companies and social media giants, those organisations and European data protection supervisory authorities have been testing and exploring the regulatory boundaries of AI during 2024. For example, the Irish DPC recently welcomed X's agreement to suspend processing of certain personal data for the purpose of training its AI chatbot tool, Grok.[10] This comes after the Irish DPC issued suspension proceedings against X in the Irish High Court noting when they did, that this was the first time that any Lead Supervisory Authority had taken such an action. Coupled with the Clearview AI investigation by the Dutch DPA, European regulators have signalled a more assertive approach to enforcement during 2024 to ensure that AI training, deployment and use remains within the guard rails of the GDPR.[11]

With thanks to the many different contributors and supervisory authorities who make this survey possible[12], our seventh annual survey takes a look at key GDPR metrics across the European Economic Area ("**EEA**") and the UK[13] since GDPR first applied and for the current year to 27 January 2025. The EEA includes all 27 Member States of the European Union plus Norway, Iceland and Liechtenstein.

"European regulators have signalled a more assertive approach to enforcement during 2024 to ensure that AI training, deployment and use remains within the guard rails of the GDPR."

8 See: https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition

9 See: https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

10 See: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-welcomes-conclusion-proceedings-relating-xs-ai-tool-grok

11 The European Data Protection Board ("**EDPB**") has recently issued an Opinion on AI models, emphasising that while AI technologies create many opportunities and benefits across a wide range of sectors and social activities, responsible AI innovation must ensure personal data are protected and in full respect of the GDPR. See: https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en#:~:text=The%20EDPB%20wants%20to%20support,case%20basis%20by%20the%20DPAs.

12 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.

13 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 has proposed legislative changes to UK data protection laws and has published the Data (Use and Access) Bill ("**DUAB**"). Although the DUAB comes with some bold statements from the Government that it will "*unlock the power of data to grow the economy and improve people's lives*", the proposals represent incremental reform, rather than radical change from the EU GDPR, with some of the more innovative elements (around smart data access and use) still unclear as we await the detail of secondary legislation.

Summary and key findings

Continued trend of sizable fines

With multiple fines issued in the hundreds of millions of Euros in previous years, data protection supervisory authorities now have more precedent to rely on and have demonstrated during 2024 their increasing confidence and willingness to impose high fines. The Irish DPC has had another busy year issuing a fine of EUR310m (USD326m/GBP257m) against LinkedIn in October 2024[14] and a fine of EUR251m (USD264m/GBP208m) against Meta in December 2024.[15] In August 2024, the Dutch DPA issued a fine of EUR290m (USD305m/GBP241m) against a well-known ride-hailing app in relation to transfers of personal data to a third country.[16]

In contrast, in November 2024, the UK Information Commissioner John Edwards was quoted as saying "*I don't believe that the quantum or volume of fines is a proxy for impact. I actually don't believe that approach is necessarily the one that has the greatest impact.*"[17] Edwards argued that issuing large fines would only tie up his office in litigation for years and that he preferred engaging with industry to ensure compliance. This is certainly an outlier approach compared with the rest of Europe and has been criticised by privacy activists. In any event, multinationals with a footprint covering the UK and the European Union will be exposed to the risk of higher fines, irrespective of the approach taken by the UK regulator.

Fall in value of annual aggregate fines imposed

For the year commencing 28 January 2024 supervisory authorities across Europe issued[18] a total of EUR1.2bn (USD1.26bn/GBP996m) in fines. In contrast to the increases of previous years, this is a decrease of 33% compared to the EUR1.78bn (USD1.87bn/GBP1.48bn) issued during the year commencing 28 January 2023. The decrease is in part due to the 2023 figures being skewed by the huge fine imposed by the Irish DPC on Meta in 2023 for EUR1.2bn (USD1.26bn/GBP996m). There was no equivalent record breaking fine this year. There have also been successful appeals across various jurisdictions, resulting in a number of fines being successfully overturned.[19] As with previous years, there is a continued trend of the biggest fines being imposed against big tech and social media giants; with nine out of ten of the top ten individual fines being imposed against organisations in this sector. However, other sectors are not out of the reach of regulators, with jurisdictions such as Italy and Spain issuing a high volume of fines across a variety of sectors.[20]

14 See: https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million

15 See: https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million

16 See: https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us

17 Article in The Times© "Big fines on tech companies are counter-productive, says regulator" 18 November 2024. The article is available (behind a paywall) here: https://tinyurl.com/5y7vj9x6

18 Not all supervisory authorities publish details of fines. Some treat them as confidential. Our survey 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.

19 For example, the total value of GDPR fines issued in Sweden has reduced from the previous figure reported in last year's survey due to successful appeals.

20 For example, as set out above, there have been a number of fines issued against organisations within the financial services sector, utility sector and healthcare sector.

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, with Ireland remaining in the top spot, with fines now totalling EUR3.5bn (USD3.7bn/GBP2.9bn). The Irish DPC has issued eight of the top ten fines to date. As predicted in last year's report, given Ireland's popularity as a European headquarters for data driven social media and big tech businesses and the fact that the Irish DPC is therefore frequently the lead supervisory authority for all cross-border processing throughout the EU, it is unsurprising that Ireland has retained the top spot for fines this year. Luxembourg is still in second place of the country league table this year with fines totalling EUR746.38m (USD784m/GPB619m),[21] primarily due to the large fine of EUR746m (USD783m/GPB619m) imposed against a US online retailer and e-commerce platform in 2021 (which is still subject to an ongoing appeal). The aggregate total fines reported since the application of GDPR on 25 May 2018 to 10 January 2025 across all jurisdictions surveyed now stands at EUR5.88bn (USD6.17bn/GBP4.88bn).

Number of breach notifications made continue to level off

In last year's survey, we saw a levelling off in data breach notifications. This trend has continued with only a small increase in the average number of breach notifications per day from 28 January 2024 to 27 January 2025, with 363 breach notifications per day compared to 335 during the same period last year.[22] This is consistent with the trend we have seen in previous years, and is likely indicative of organisations becoming more wary of reporting data breaches given the risk of investigations, enforcement, fines and compensation claims that may follow notification.

A recurring theme of DLA Piper's previous annual surveys is that there has been little change at the top of the tables regarding the total number of data breach notifications made since the GDPR came into force on 25 May 2018 and during the most recent full year from 28 January 2024 to 27 January 2025. The Netherlands, Germany,[23] and Poland remain in the top three spots for the highest number of data breaches notified from 28 January 2024 to 27 January 2025, with 33,471; 27,829, and 14,286 breaches notified respectively.

21 The fine is not publicly available and is still subject to an ongoing appeal.

22 Not all the countries covered by this survey make breach notification statistics publicly available and many provided data for only part of the period covered by this survey. 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. As a number of data protection supervisory authorities have now issued annual reports for 2023, some figures in last year's survey that were previously extrapolated have been updated in this survey.

23 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

In May 2023, the Irish DPC imposed a record administrative fine of EUR1.2bn (USD1.26bn/GBP996m) against Meta[24], 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 EEA personal data transferred to the US in violation of GDPR. At issue in the inquiry underlying the Irish DPC's decision was whether Meta's transfers of EEA personal data to the US, based on Standard Contractual Clauses ("**SCCs**") and supplementary measures as recommended by the European Data Protection Board ("**EDPB**"), were legal following the Schrems II judgment.[25] In its decision, the Irish DPC concluded that Meta's reliance on the new 2021 SCCs did not compensate for the deficiencies in US law identified in Schrems II – given that Meta could not stop access by US public authorities with the SCCs and as there was no remedy for an EEA data subject whose data were accessed. In addition, the DPC concluded that Meta did not have any supplemental measures in place which would compensate for the inadequate protection provided by US law.

Luxembourg's data protection supervisory authority, the CNPD, continues in second position this year with a fine of EUR746m (USD783m/GPB619m) against a US online retailer and e-commerce platform. The fine is not publicly available and is subject to an ongoing appeal.

On 2 September 2022, the Irish DPC imposed a fine of EUR405m (USD425m/GBP336m)[26] on Meta (in relation to Instagram). The Irish DPC found that Meta, among 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 the contact information data.

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

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

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

Spotlight on personal liability

The issue of personal liability in relation to breaches of the GDPR was raised in a recent decision by the Dutch DPA. In September 2024, the Dutch DPA issued a fine of EUR30.5m (USD32.03m/GBP25.32m) against the facial recognition software provider, Clearview AI.[27] Clearview AI collected images of people's faces and data from publicly available information on the internet and social media platforms around the world and provided an online global database that could be used for facial recognition, allowing its customers to check images against all the images in the database. Individuals were not informed that their personal data was used in this way and the database contained a substantial amount of data.

Following a series of complaints dating back to May 2021 by privacy activists and other digital rights organisations, several data protection supervisory authorities issued monetary penalties against Clearview AI for breaches of GDPR.

As Clearview AI has faced a raft of GDPR penalties over the last few years[28] but continues to operate in the same way, the Dutch DPA also ordered incremental penalties of up to EUR5.1m (USD5.4m/GBP4.2m) to be issued for continued non-compliance, stating that Clearview AI had failed to stop the GDPR violations after the investigation concluded and, in an unprecedented move, stated that it is investigating whether it can "*hold the management of the company personally liable and fine them for directing the violations*". The Dutch DPA was clear that "*this liability already exists if directors know that the GDPR is being violated, have the authority to stop that, but omit to do so, and in this way consciously accept those violations*". This signals a potential shift in focus by European data protection supervisory authorities to hold management personally liable for failures to comply with GDPR requirements.

With several of the new laws and regulations forming part of the EU Digital Decade also creating personal liability for management bodies, we anticipate a greater focus on the personal liability of individuals and more enforcement where their oversight is found wanting.

"2024 is the year when GDPR enforcement got personal."

27 See: https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition

28 Including from the Italian supervisory authority (see: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323), the French supervisory authority (see: https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en) and the Greek Data Protection Authority (see: https://www.homodigitalis.gr/wp-content/uploads/2022/07/HellenicDPA_ClearviewDecision_13.7.2022_.pdf)

Commentary

The aggregate value of fines issued across the countries surveyed has decreased this year from EUR1.78bn (USD1.87bn/GBP1.48bn) issued in the year from 28 January 2023 to EUR1.2bn (USD1.26bn/GBP996m) in fines in the year from 28 January 2024. European data protection authorities have nevertheless issued a number of large fines this year and it is worth noting that two thirds of the previous year's higher aggregate total fines issued was made up of a single fine issued by the Irish DPC against Meta.[29] The clear trend is for more frequent and higher fines as regulators gain confidence and assertiveness. With yet another large fine of EUR251m (USD264m/GBP208m) issued this year by the Irish DPC against Meta, as well as a fine of EUR310m (USD326m/GBP257m) issued against LinkedIn, Ireland is firmly in the top spot for the total value of GDPR fines imposed, with aggregate fines totalling EUR3.5bn (USD3.7bn/GBP2.9bn). However, the majority of the top ten fines issued by the Irish DPC are still making their way through the appeal process so it is still possible that some will be overturned or reduced. The Dutch DPA also issued two of its largest fines to date during 2024 with a fine against a well-known ride-hailing app of EUR290m (USD305m/GBP241m) in relation to transfers of personal data to a third country[30] and a fine of EUR30.5m (USD32.03m/GBP25.32m) against the facial recognition software provider, Clearview AI.[31]

GDPR fines: just an issue for big tech?

Given the headline grabbing fines issued in recent years by European data protection supervisory authorities against big tech and social media giants, organisations in other sectors could be excused for thinking that the focus of regulators is solely on Silicon Valley. However, it is evident that other sectors are not beyond the reach of regulators. While some supervisory authorities, like those in Ireland and Luxembourg, have chosen to issue a small number of large, high-profile fines, in contrast, others, such as those in Italy and Spain, have opted to issue many more fines, often for smaller amounts, against organisations in a broad range of different sectors. In particular, 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 and across all sectors, in particular in relation to the healthcare sector, energy sector and financial services sector.[32]

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

30 See: https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million

31 See: https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition

32 Ibid.

There is ongoing debate about the best enforcement approach by European data protection supervisory authorities. Large fines can attract media attention and deter violations but require significant resources to manage, especially against large, well-resourced multinationals and as the UK ICO has commented publicly this year, the appeal process can last years and consume much of the regulator's limited resources. Successful appeals or reductions in fines can also weaken the enforcement process and its deterrent effect and undermine the effectiveness and confidence of investigation and enforcement teams in data protection authorities. The alternative approach of fining little and often, preferred by supervisory authorities in countries such as Italy and Spain, typically does not generate the same media interest but also results in fewer appeals. Organisations across all sectors are more likely to be fined for GDPR infringements in Spain and Italy relative to other countries surveyed, albeit the quantum of the fines issued are typically much lower than the headline grabbing fines issued by the Irish DPC.

It is notable that a finding of a breach of the GDPR by a specialist data protection authority not only risks fines or sanctions being imposed by that authority but also makes it easier for individual data subjects and contractual counterparties to bring claims for compensation and other contractual remedies. While technically a claimant will still need to prove a breach of the GDPR in the courts, the courts are typically reluctant to second guess findings of breach of the GDPR by a specialist data protection authority.

While some organisations may welcome the alternative approach proposed by the UK ICO of the regulator engaging with industry rather than imposing headline making fines, it seems unlikely that this approach will catch on in the rest of Europe.

Enforcement trends

Continued focus on the pre-eminence of the lawfulness, fairness and transparency principle

This year has seen a continuation of last year's enforcement trends with multiple fines issued by data protection supervisory authorities for breach of the lawfulness, fairness and transparency principle (Article 5(1)(a) GDPR). For example, the Irish DPC fined LinkedIn EUR310m (USD326m/GBP257m)[33] for a number of infringements of the GDPR in relation to the lawfulness, fairness and transparency of processing. The decision came after the Irish DPC initiated an inquiry based on an initial complaint submitted through the French Data Protection Authority. The Irish DPC led the investigation in its role as the lead supervisory authority for LinkedIn, as LinkedIn's EU business operations are headquartered in Ireland. The inquiry examined LinkedIn's processing of personal data for the purposes of behavioural analysis and targeted advertising of users who had created LinkedIn profiles and related to the processing of personal data provided directly by LinkedIn members and data obtained from third-party partners related to LinkedIn members.

Various breaches of the lawfulness, fairness and transparency principle were identified by the Irish DPC including: that the consents obtained by LinkedIn to legitimise the processing of third party data of its members for the purpose of behavioural analysis and targeted advertising were invalid as they were not freely given, sufficiently informed, specific, or unambiguous; that there was no contractual necessity (Article 6(1)(b) GDPR) for the processing of relevant data; that LinkedIn was also unable to rely on legitimate interests (Article 6(1)(f)GDPR), as LinkedIn's interests "*were overridden by the interests and fundamental rights and freedoms of data subjects*", and that LinkedIn was in breach of the more specific transparency requirements set out in Articles 13(1)(c) and 14(1)(c) GDPR.

33 See: https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million Please note that the full decision has not yet been published by the Irish DPC.

Similarly, in the Czech Republic, the Czech Office for Personal Data Protection ("**Czech DPA**") imposed a fine of approximately EUR14m (USD14.7m/GBP11.6m) on Avast Software, after investigating the company's Czech branch, Jumpshot, INC. In 2019, Avast transmitted pseudonymized internet browsing history, linked to unique identifiers, of approximately 100 million users to Jumpshot, Inc. The Czech DPA determined that Jumpshot provided this user data to marketers to gain insights into online consumer behaviour and track user journeys. They determined that users were wrongly informed by Avast about the transfer of anonymous data for the purpose of trend analysis and that the transmitted data from individual antivirus software installations was not anonymized and data subjects could in fact be re-identified. In addition, they determined that the purpose of processing the data was not solely to create statistical analyses, as claimed by Avast, but also for the purpose of tracking online consumer behaviour for which Avast had no lawful basis.

Breach of the integrity and confidentiality principle

Continuing the trend of last year, this year has also seen multiple fines issued by data protection supervisory authorities for breach of the integrity and confidentiality principle (Article 5(1)(f) GDPR) and the related obligation to ensure security of processing personal data (Article 32 GDPR).

For example, in Italy, the Italian Garante imposed a fine of EUR6.4m (USD6.7m/GBP5.3m) on Eni Plenitude S.p.A. for, among other breaches, failing to implement appropriate security measures[34]. In Greece, the Hellenic Data Protection Authority ("**Greek DPA**") imposed a fine of EUR2.96m (USD3.1m/GBP2.46m) on Hellenic Post S.A. ("**ELTA**"), for failing to implement appropriate technical and organisational measures to secure personal data, after ELTA reported two breach incidents to the Greek DPA. The first incident involved a malicious cyber-attack leading to the encryption of the company's systems and the demand of a ransom. The second incident involved a cyber-attack leading to the exfiltration of some of the company's data which was subsequently published on the Dark Web.[35]

In Ireland, the Irish DPC imposed a fine of EUR251m (USD264m/GBP208m) against Meta, following a personal data breach, first reported by Meta in September 2018.[36] The data breach, caused by exploitation by unauthorised third parties of user tokens on Meta's Facebook platform, impacted approximately 3 million Facebook users in the EEA and included special categories of personal data and children's personal data. Among other breaches, the Irish DPC found that Meta had failed to include all of the information required by Article 33(3) GDPR in its breach notification. They also found that Meta had failed to document the facts relating to each breach, the steps taken to remedy them, and to do so in a way that would allow the compliance to be verified by the regulator (in breach of Article 33(5) GDPR). The Irish DPC further found that Meta had breached Article 25(1) GDPR, by failing to ensure that data protection principles were protected in the design of processing systems, and Article 25(2) GDPR, by failing in their obligations as controllers to ensure that, by default, only personal data that are necessary for specific purposes are processed.

34 See: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10029424

35 See: https://www.edpb.europa.eu/news/national-news/2024/hellenic-sa-fine-company-failure-implement-technical-and-organisational_en

36 See: https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million

Looking back at our predictions for 2024

In last year's report we predicted that there would be more regulatory enforcement, appeals and litigation relating to the "grand bargain" funding the Internet, namely online service providers relying on harvesting user information to generate revenues from behavioural advertising to fund "free" consumer services, commonly referred to as the "consent or pay" model. We also predicted more bumps in the road for data transfers and the latest incarnation of the EU-US adequacy decision, and more complaints, investigations and enforcement activity in relation to cookies and similar tracking technologies, AI and shortcomings in governance and oversight.

Consent or pay model

The "consent or pay" model has been the subject of lively debate among European data protection supervisory authorities and complaints from privacy activists. In January 2024 the Dutch DPA in its own capacity and also acting on behalf of the Norwegian and German (Hamburg) data protection supervisory authorities requested a formal opinion from the EDPB on "consent or pay" models and their legality when used by large online providers. The EDPB adopted their opinion in April 2024.[37]

The EDPB concluded that offering the option to access a service without having to share personal data for behavioural advertising purposes in consideration of a fee, should not be the default approach for large online platforms. Individuals should be provided with an "equivalent alternative" that does not require a fee. The EDPB further stated that if large online platforms choose to charge a fee for access to the equivalent alternative, they should also offer a "*further alternative, free of charge, without behavioural advertising*" – the EDPB considered this to be "*a particularly important factor*" when assessing whether consent is valid under GDPR. Individuals must have a genuine free choice, and any fee charged should not make them feel compelled to consent.

In the opinion, the EDPB confirmed that, when assessing whether consent is "freely given", controllers should consider: "*whether the data subject suffers detriment by not consenting or withdrawing consent; whether there is an imbalance of power between the data subject and the controller; whether consent is required to access goods or services, even though the processing is not necessary for the fulfilment of the contract (conditionality); and whether the data subject is able to consent to different processing operations (granularity)*".

The EDPB confirmed that controllers should assess, on a case-by-case basis, whether imposing a fee for a service is appropriate and, if so, the amount of that fee. In particular, large online platform controllers should ensure that the fee does not inhibit data subjects from making a genuine choice in light of the requirements of valid consent and the principle of fairness under Article 5(1)(a) GDPR.

The application of the opinion is specifically limited to use of consent or pay models by large online platforms. The rationale stated for limiting the scope of the opinion in this way is that large online platforms attract large amounts of users in the EEA; conduct large scale processing; have a dominant position in the market and therefore *"may be uniquely situated in respect of some of the criteria for valid consent, e.g. in respect of the existence of an imbalance of power"*.

37 See: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en

The EDPB opinion raises the question as to how online services will be paid for if large online service providers are unable to obtain valid consent for the harvesting and monetisation of consumers' personal data. Although the EDPB does not go as far as prohibiting the use of a "consent or pay" model for behavioural advertising purposes, stating only that these models will not satisfy the requirements of valid consent under the GDPR "in most cases", it sets a very high bar for the "consent or pay" model to be lawful. In the press release accompanying the opinion, the Chair of the EDPB, Anu Talus commented: "*Controllers should take care at all times to avoid transforming the fundamental right to data protection into a feature that individuals have to pay to enjoy. Individuals should be made fully aware of the value and the consequences of their choices.*" If personal data cannot be harvested by large online platforms to sell to advertisers to generate the revenues needed to fund innovative consumer services, it begs the question, will consumers thank the EDPB if these popular services are curtailed or stopped in Europe as a result of the EDPB's strict interpretation of GDPR? Meta has previously threatened in its annual report[38] to shut down Facebook and Instagram in Europe over European privacy laws and enforcement action. If consumers are faced with a choice between their fundamental right to data protection or being able to continue to access their social media accounts for free, would they really choose data protection?

In June 2024, Meta filed a lawsuit against the EDPB at the General Court of the European Union, challenging the EDPB's opinion on 'consent or pay' models.[39] Among other arguments, Meta alleged that the EDPB's opinion constitutes *"an illegal and disproportionate interference"* with Article 16 of the Charter of Fundamental Rights of the European Union ("**Charter**"), which protects the freedom to conduct a business. Meta argued that the opinion fails to strike a fair balance between conflicting fundamental rights. In addition, Meta also alleged that the opinion introduces "*a novel and incoherent obligation that is nowhere to be found in the GDPR*", in violation of Article 52(1) of the Charter, the principle of legal certainty, the notion of consent (Article 4(11) GDPR), and the principle of data minimisation (Article 5(1)(c) GDPR).

38 See: https://www.sec.gov/Archives/edgar/data/1326801/000132680123000013/meta-20221231.htm

39 See: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202404865

Transfers

Transfers of personal data to third countries outside of the EEA continue to attract regulatory attention. For example, a fine of EUR290m (USD305m/GBP241m) was issued by the Dutch DPA against a well-known ride-hailing app in relation to transfers of personal data to a third country.[40] In its decision, the Dutch DPA stated that the company had failed to appropriately safeguard transfers of personal data from the EU to the U.S. The Dutch DPA found that after the invalidation of the EU-US Privacy Shield, the company had only put SCCs in place until August 2021. After that point, the Dutch DPA stated that no valid mechanism was in place to appropriately safeguard the transferred personal data, in breach of Chapter V GDPR, until 21 November 2023, the date on which the company was included on the Data Privacy Framework ("**DPF**") list.

In response to the Dutch DPA's questions, the company explained that it had previously entered into the legacy controller-to-controller standard contractual clauses. However, when the new SCCs were approved by the European Commission in 2021, it had removed the standard contractual clauses in its data sharing agreement, arguing that it followed the European Commission's FAQs – which state that the new SCCs can only be used for data transfers where the data importer is not subject to GDPR and "*do not work for importers whose processing operations are subject to the GDPR pursuant to Article 3, as they would duplicate and, in part, deviate from the obligations that already follow directly from the GDPR*". The decision by the Dutch DPA seems to directly contradict the European Commission's statement, published at a time when there was considerable uncertainty and a lack of clarity around transfers of personal data to third countries. It's clear that transfers of personal data to third countries outside of the EEA are still attracting attention from both privacy activists and EU regulators, as well as large financial penalties. In an apparent reaction to the decision, the European Commission has published plans to launch a public consultation on standard contractual clauses which aim to address the specific scenario where the data importer is located in a third country but is directly subject to the GDPR.

Last year, we also predicted that there would be some bumps in the road for the EU-US Data Privacy Framework.[41] As mentioned in our previous report, the NGO Noyb (My Privacy is None of Your Business), which led the previous legal challenges to both Privacy Shield and Safe Harbor, announced that it will also challenge the DPF. Schrems III still seems to be on the horizon. In 2024, the Irish High Court, gave Mr Schrems approval to participate in Meta's legal challenge against the Irish DPC's decision requiring the suspension of user data transfers from Europe to the US and the subsequent EUR1.20bn (USD1.25bn/GBP997m) fine.[42]

As an illustration of just how challenging it is to achieve compliance with the international data transfer restrictions in Chapter V GDPR, on January 8, 2025 the European General Court set a novel precedent by ordering the European Commission to pay EUR400 (USD420/GBP332) damages to an individual after their personal data were determined to have been unlawfully transferred by the European Commission to the US.[43]

40 See: https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us

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

42 See: https://www.irishtimes.com/business/2024/02/15/high-court-permits-privacy-campaigner-to-participate-in-metas-challenge-to-data-transfer-suspension/

43 Judgment of the General Court in Case T-354/22 | Bindl v Commission. See press release here: https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-01/cp250001en.pdf

Cookies and similar tracking technologies

Earlier this year, the CJEU ruled on various questions referred by the Austrian courts in relation to Mr Schrems' action challenging the processing of his personal data by Meta in the context of the online social network Facebook. Mr Schrems had argued that personal data relating to his sexuality had been processed unlawfully by Meta to send him personalised advertisements.[44] He further alleged that this processing took place without his consent or other lawful basis under the GDPR. In its judgment, the CJEU held that Art. 5(1)(c) GDPR does not allow the controller, in particular a social network platform, to process data collected inside and outside the platform for the purpose of personalised advertising for unlimited time and without distinction as to the type of data. The CJEU emphasised that the principle of data minimisation requires the controller to limit the retention period of personal data to what is strictly necessary in the light of the objective of the processing activity. Regarding the collection, aggregation and processing of personal data for the purposes of targeted advertising, without distinction as to the type of those data, the CJEU held that a controller may not collect personal data in a generalised and indiscriminate manner and must refrain from collecting data which are not strictly necessary for the processing purpose. The CJEU also held that the fact that an individual manifestly made public information concerning their sexual orientation does not mean that the individual consented to processing of other data relating to their sexual orientation by the operator.

Last year we referred to the EDPB's consultation on draft guidelines on the scope of Article 5(3) of the e-Privacy Directive – i.e. the so-called "cookie rule"[45]. In October 2024, the EDPB adopted the updated guidelines on the scope of Article 5(3).[46] These guidelines are very similar to the original draft adopting a broad interpretation of the cookie rule, meaning that a wide variety of technologies that were not obviously caught by Article 5(3) are caught, at least in the opinion of the EDPB. The EDPB guidelines are not legally binding and it will be up to the courts to decide whether the EDPB has overstepped in its broad interpretation of Article 5(3).

44 See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0446

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

46 See: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf

AI

Last year, we predicted that there would be continued investigations and enforcement into AI using personal data to train or enhance AI systems and solutions. Again, this prediction has come to pass, with the most recent fine of EUR30.5m (USD32.03m/GBP25.32m) against Clearview AI issued by the Dutch DPA.[47] In Ireland, the Irish DPC welcomed X's agreement to suspend its processing of certain personal data for the purpose of training its AI chatbot tool, Grok, after the Irish DPC issued suspension proceedings against X in the Irish High Court. Section 134 of the (Irish) Data Protection Act 2018 allows the Irish DPC, where it considers there is an urgent need to act to protect the rights and freedoms of data subjects, to make an application to the High Court for an order requiring a data controller to suspend, restrict, or prohibit the processing of personal data. The High Court proceedings were issued as a result of a complaint to the Irish DPC raised by consumer rights organisations Euroconsumers and Altroconsumo on behalf of data subjects in the EU/EEA. The complainants argued that the Grok chatbot was being trained with user data in a manner that did not sufficiently explain the purposes of data processing, and that more data than necessary was being collected. They further argued that X may have been handling sensitive data without sufficient reasons for doing so. Much of the complaint stemmed from X's initial approach of having data sharing automatically turned on for users in the EU/EEA, which it later mitigated by adding an opt-out setting. X claimed that it had relied on the lawful basis of legitimate interest under the GDPR, but the complainants argued that X's privacy policy – dating back to September 2023 – was insufficiently clear as to how this applied to the processing of user data for the purposes of training AI models such as Grok.

This development followed a similar chain of events involving Meta in June. Complaints from the NGO Noyb were made against Meta's reliance on "legitimate interest" in relation to the use of data to train AI models. This led to engagement with the Irish DPC and the eventual decision in June by Meta to pause relevant processing (without the need for the authority to invoke Section 134).[48] The fact that much of the high profile activity relating to regulation of AI is coming from the data protection sphere will no doubt bolster the EDPB's recommendation in a statement in July 2024 that Data Protection Authorities ("**DPAs**") are best placed to regulate high risk AI.[49]

In Italy, the Italian Garante issued a significant ruling addressing breaches of the GDPR by an AI-powered chatbot.[50] The investigations by the Garante were triggered following a data breach suffered by the chatbot in 2023. Following the investigation the Italian Garante issued a fine of EUR15m (USD15.75m /GBP12.45m) against the company. The Italian Garante noted that, among other breaches, the company failed to notify the breach in a timely manner, as required under Article 33 GDPR, despite the breach's potential to cause significant risks to affected individuals. It highlighted that since, at the time of the events, the company had no establishment in the EU, it had to notify the data breach to all the EU data protection authorities whose residents had been affected as it had no lead supervisory authority at that time.

The Italian Garante also found that the company breached Articles 5(2) and 6 GDPR for failing to identify a valid legal basis for processing personal data to train its AI model before launching the service. In addition, the Italian Garante held that the company had breached Articles 5(1)(a), 12, and 13 GDPR due to significant deficiencies in its privacy policy. The issues primarily related to a lack of transparency, accessibility, and completeness in the information provided about how personal data was processed, especially for training AI models.

47 See: https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition

48 See: https://www.dataprotection.ie/en/news-media/latest-news/dpcs-engagement-meta-ai

49 See: https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf

50 See: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432#english

These decisions signal the intent of data protection supervisory authorities to closely scrutinise the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate GDPR compliance into the core design and functionality of their AI systems.

In December 2024, the EDPB adopted its much anticipated opinion on the lawful use of personal data for the development and deployment of AI models.[51] The opinion aims to provide guidance on the processing of personal data in the context of AI model development and deployment and was issued in response to a specific request from the Irish DPC. The opinion focuses on four key issues: (1) under what circumstances may an AI Model be considered as 'anonymous; (2) how controllers may demonstrate the appropriateness of legitimate interest as a legal basis for personal data processing to create, update and/or develop an AI Model; (3) how controllers may demonstrate the appropriateness of legitimate interest as a legal basis for personal data processing to deploy an AI Model, and (4) what are the consequences of an unlawful processing of personal data in the development phase of an AI model on the subsequent processing or operation of the AI model.

As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services by big tech players, amongst others, to enrich data. This is particularly the case where it is perceived that data sets are being re-purposed and further processing is taking place. In such circumstances, it is essential that an appropriate legal basis is being relied upon – noting the significant issues that can arise if there is an over-reliance on legitimate interest. The Irish DPC and other regulators are likely to investigate, engage and ultimately intervene where they believe that data subjects' rights under the GDPR are threatened. Perhaps in anticipation of more cross-border enforcement activity concerning AI, last month, the European Commission proposed a new law to streamline cooperation between DPAs when enforcing the GDPR in such cases.[52]

Governance and oversight

As predicted in last year's report and mentioned above, European data protection supervisory authorities have continued to prioritise the importance of governance and oversight, particularly in light of the raft of new data, digital and cyber regulation forming the EU Digital Decade programme of regulation.[53] Governance frameworks are becoming increasingly important for organisations to be able to comply with specific requirements for effective governance frameworks.

51 See: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

52 See: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609

53 See: https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

Predictions for the year ahead

- The "consent or pay" model will remain in the regulatory cross-hairs during 2025. The EDPB[54] and decisions by the Irish DPC[55] have effectively closed the door to relying on contract necessity and legitimate interests as lawful bases under GDPR for the processing of personal data for behavioural advertising purposes, leaving consent as the last option. The EDPB opinion on consent or pay models used by large online platforms while not going so far as to state that these models can never be lawful, did conclude that in most cases these models do not comply with the GDPR requirements for valid consent (and therefore are unlawful). With the future of the grand bargain at stake, all eyes will be on the General Court of the European Union where Meta is challenging the findings made in the EDPB opinion.[56]
- There will be a continued focus on the personal liability of company officers and directors and other individual members of management bodies for infringements of GDPR by regulators as a lever to drive better compliance. The Dutch DPA's stated intention to investigate whether the directors of Cleaview AI can be held personally responsible for the company's alleged ongoing violations of GDPR is a high profile example and we anticipate the focus on personal liability of individual members of management bodies will continue during 2025. Whether regulators have the legal powers to impose personal liability for GDPR infringements is a question of domestic law and the position varies among Member States. Nevertheless, the statement of intent by the Dutch DPA is, we predict, the first of what we expect will be more attempts by supervisory authorities to hold officers, directors and others in management individually liable for GDPR infringements. Personal liability is a powerful lever to drive compliance.
- As the much anticipated EDPB opinion on AI models[57] does not provide many clear or definitive answers, data protection supervisory authorities and organisations developing, deploying and using AI will continue to grapple with the relationship between AI and data protection law in 2025. The boundaries of what is and is not lawful use of personal data within AI models remain far from clear. We anticipate continued investigations, enforcement actions and appeals in the coming year as the rapid deployment of AI meets strict EU data protection laws. The new Trump administration in the U.S. and comments made that it will take a more hands off approach in relation to the regulation of AI[58] makes a clash of regulatory approaches more likely, as lightly regulated US AI vendors provide services into the much more conservative and highly regulated European Union. We predict more investigations and enforcement regarding AI use during 2025.
- European data protection supervisory authorities will continue to prioritise the importance of the lawfulness, fairness and transparency principle (Article 5(1)(a) GDPR), with failures to comply with the principle consistently remaining one of the top enforcement priorities for regulators. This year we have seen a continuation of multiple fines issued by data protection supervisory authorities for breach of the lawfulness, fairness and transparency principle (including the Irish DPC's fine of EUR310m (USD326m/GBP264m)[59] against LinkedIn for a number of infringements of the GDPR in relation to the lawfulness, fairness and transparency of processing) and we predict that this principle will continue to attract close regulatory scrutiny during 2025.

54 See: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en

55 See: https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-91-million-fine-of-Meta; https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-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.

56 See: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202404865.

57 See: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

58 See: https://www.presidency.ucsb.edu/documents/2024-republican-party-platform.

- Finally, we predict that the UK will continue to take a "less is best" approach to enforcement with very few GDPR fines anticipated from the UK ICO during 2025. In addition to the comments made by the UK Information Commissioner, John Edwards, in the Times© newspaper in 2024[60] to the effect that imposing large fines is ineffective, the UK Chancellor, Rachel Reeves, has said that she wishes to reduce the regulatory burden on British businesses stating that "the UK has been regulating for risk, but not regulating for growth".[61] The UK Prime Minister has also recently stated the UK government's position in relation to AI regulation saying that the UK will "go our own way" and will "*test and understand AI before we regulate it to make sure that when we do it, it's proportionate and grounded.*"[62] In other words, with the UK government firmly focussed on growth and the UK economy stubbornly sluggish, there is little appetite for active enforcement of existing laws or more laws. While we therefore predict a quiet year with respect to enforcement of the UK GDPR, we anticipate that there will be more active enforcement of other cybersecurity laws and regulations during 2025, notably the NIS Regulations 2018, given the continuing threat and prevalence of cyber-attacks.

59 Ibid.

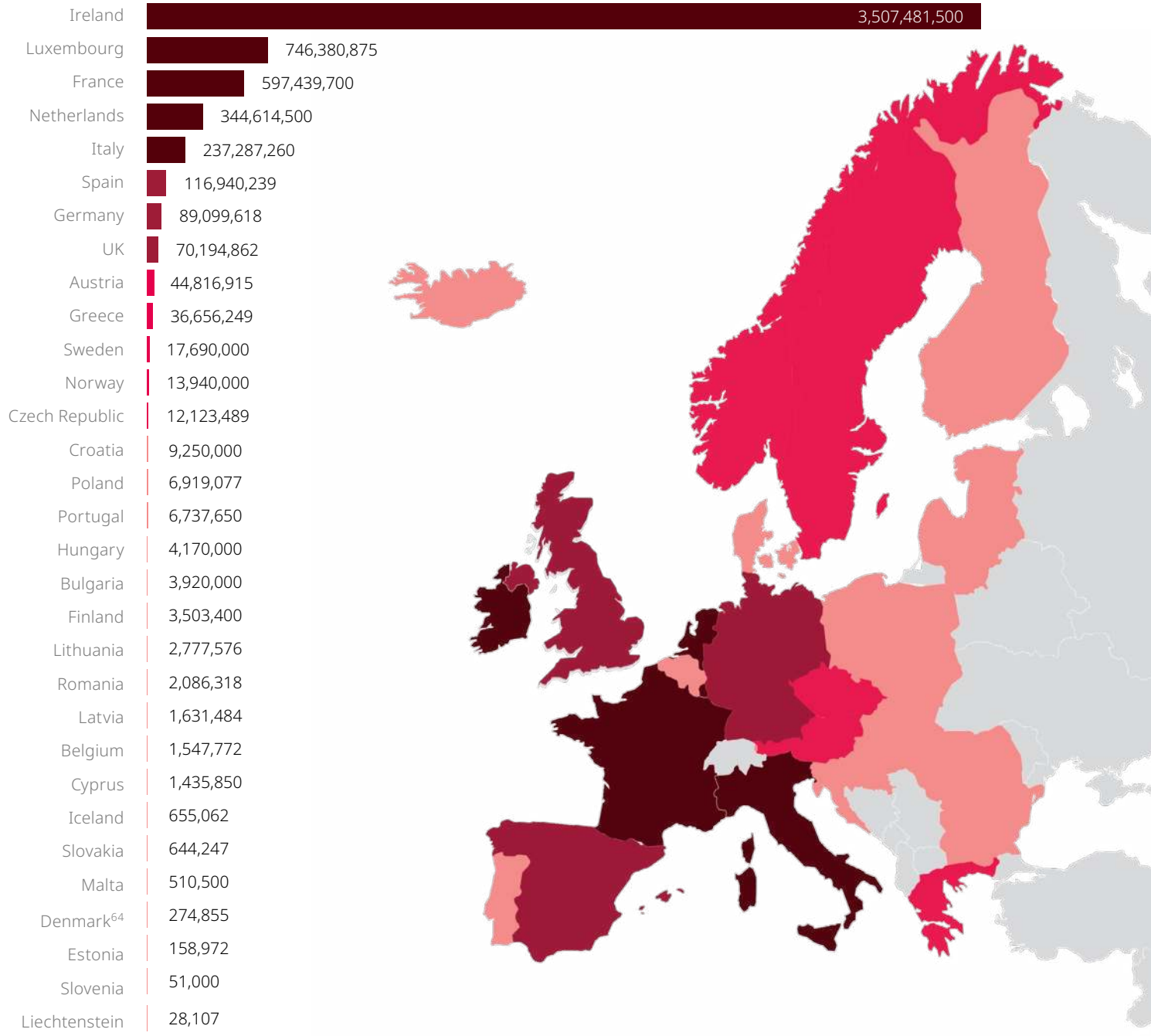
60 See: https://www.thetimes.com/business-money/companies/article/big-fines-on-tech-companies-are-counter-productive-says-regulator-bfkpc6xrk.

61 See: https://www.gov.uk/government/speeches/mansion-house-2024-speech.

62 See: https://www.gov.uk/government/speeches/pm-speech-on-ai-opportunities-action-plan-13-january-2025.

Report

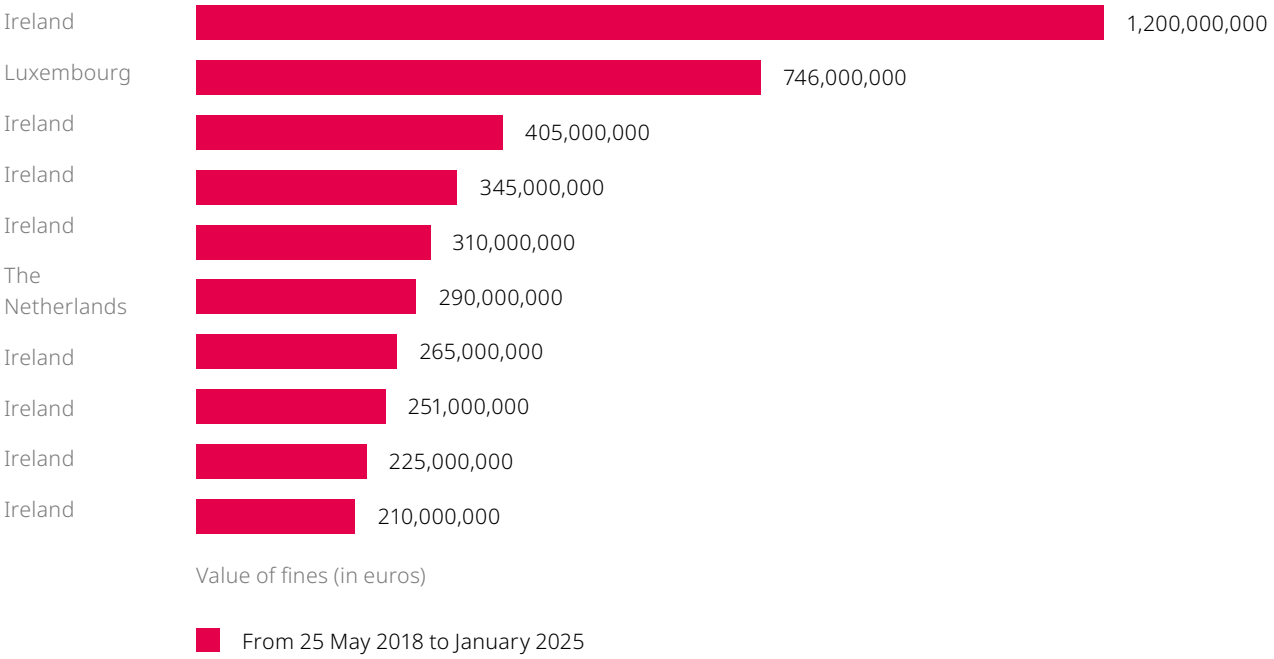
Total value of GDPR fines imposed from 25 May 2018 to date (in euros)[63]



63 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.

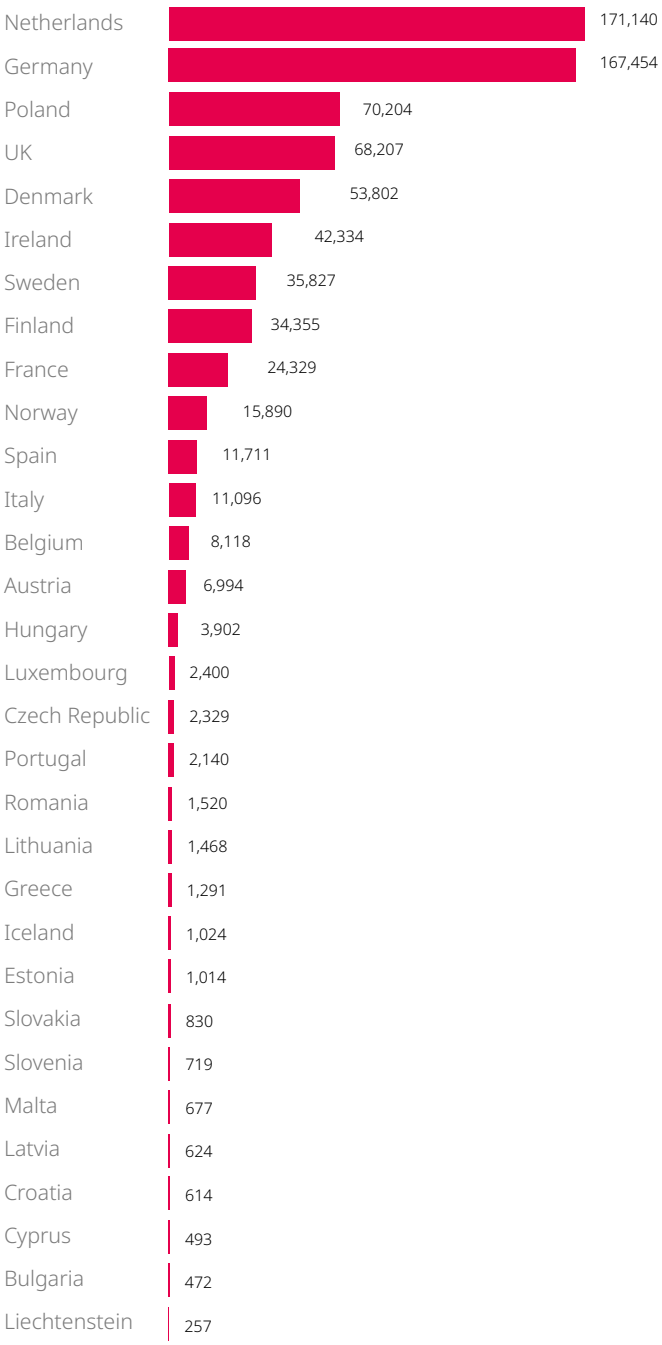
64 In Denmark, the supervisory authority ("**Datatilsynet**") does not have the authority to issue administrative fines. Instead, the Datatilsynet provides a recommendation as to the size of the fine and it is for the national courts to ultimately decide on the value of the fine imposed. In this survey, 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[65]



65 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).

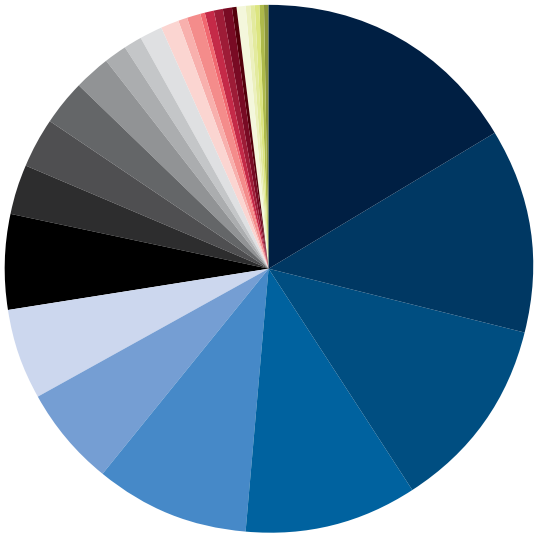
Total number of personal data breach notifications between 25 May 2018 and 27 January 2025 inclusive*



Total number of personal data breach notifications between 28 January 2024 and 27 January 2025*

* 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 2024 and 27 January 2025 (last 12 month period)	Change compared to last year's ranking*
Netherlands	**188.33**	+3
Lichstenstein	**144.98**	No change
Finland	**137.18**	+2
Denmark	**119.95**	-3
Ireland	**109.49**	-2
Norway	**67.69**	+1
Luxembourg	**65.43**	-1
Sweden	**64.47**	+12
Poland	**36.87**	No change
Iceland	**34.8**	+1
Germany	**33.08**	-3
Malta	**23.59**	+3
Estonia	**15.88**	-3
UK	**14.49**	-2
Austria	**14.29**	-2
Belgium	**12.6**	No change
Lithuania	**8.38**	-3
France	**6.4**	-1
Spain	**6.32**	+5
Slovenia	**6**	-2
Cyprus	**5.59**	+1
Hungary	**5.38**	-3
Latvia	**5.01**	-2
Italy	**3.94**	+2
Slovakia	**3.59**	+2
Czech Republic	**3.32**	-1
Portugal	**3.13**	-4
Croatia	**2.38**	No change
Greece	**2.14**	No change
Bulgaria	**0.56**	No previous data
Romania	**0.34**	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 2024 estimates).

* Full breach notification statistics were not, at the time of publication, publicly available for 2024 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 2023, this may have impacted upon last year's rankings. In some jurisdictions, 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.

Navigating the Digital Decade

With the rise in new and proposed laws and regulations applying to data and the digital world, governance and effective risk management are essential for organisations to be able to tackle legal complexity and compliance risk, and to ensure business continuity. We have a dedicated *Digital Decade website*, to provide insights and keep you up to date with developments. We have also designed a Digital Decade control framework, providing a method to simplify implementation of Digital Decade initiatives, using a clear, defensible, pragmatic framework. The control framework provides a standardised approach for translating key legislative obligations into practical controls, mapped to applicable standards, proposing a series of predefined descriptions of gaps and measures to close the gaps.

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 200 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 300 organisations to assess exports of personal data from the UK and EEA to third countries and we now have over 80 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.

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com