A REPORT BY DLA PIPER'S DATA, PRIVACY AND CYBERSECURITY TEAM
JANUARY 2026

GDPR fines and data breach survey

DLA PIPER

DLA Piper GDPR fines and data breach survey

Enforcement activity has remained high this year, with the aggregate value of GDPR fines across all surveyed countries reaching a figure comparable to last year, at approximately EUR1.2bn (USD1.42bn/GBP1.06bn).[1] Ireland once again remains the top enforcer by highest aggregate GDPR fines since 25 May 2018, with the Irish Data Protection Commission ("**DPC**") imposing fines totalling EUR4.04bn (USD4.77bn/GBP3.56bn) to date – a significant gap from second place France with fines totalling EUR1.1bn (USD1.3bn/GBP968m),[2] and third place Luxembourg, with fines totalling EUR746.56m (USD880.94m/GBP656.97m), primarily due to the large fine imposed against a US online retailer and e-commerce platform, which was upheld by Luxembourg's Administrative Court in March 2025.[3] The total fines reported across all surveyed countries since the application of GDPR in 2018 now stands at EUR7.1bn (USD8.4bn/GBP6.2bn). Despite an active year with significant fines imposed, the largest fine ever imposed remains the EUR1.2bn (USD1.42bn/GBP1.06bn) issued against Meta Platforms Ireland Limited ("**Meta IE**") in 2023.[4]

GDPR compliance risks extend beyond regulatory penalties. There is also the potential for follow-on compensation claims. This year has brought several notable rulings from the Court of Justice of the European Union ("**CJEU**") and European courts on GDPR-related compensation - particularly regarding the criteria for pursuing claims for non-material damage.

With thanks to the many different contributors and supervisory authorities who make this survey possible,[5] our eighth annual survey takes a look at key GDPR metrics across the European Economic Area ("**EEA**") and the UK[6] since GDPR first applied and for the current year to 28 January 2026. The EEA includes all 27 Member States of the European Union plus Norway, Iceland and Liechtenstein.

"2025 saw a 22% year on year increase in data breach notifications. This reflects a widely reported increase in malicious cyber attacks amid heightened geopolitical tensions."

1 In this survey we have used the following exchange rates: EUR1 = USD1.18/GBP0.88. 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. In addition, in most jurisdictions, fines have been successfully appealed which may impact the total aggregate fine figures. When quoting findings of data protection supervisory authorities within this survey, DLA Piper is not endorsing any of those findings of law or fact

2 In France, when collating data, it is not possible to separate the fines imposed under the GDPR and those imposed under other regimes, such as e-privacy legislation. Therefore the aggregate value of fines imposed under the GDPR in France may be inflated

3 See the press release from the Luxembourg data protection supervisory authority: https://cnpd.public.lu/fr/actualites/national/2025/03/amazon-decision.html

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

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 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). On 19 June 2025, the UK Data (Use and Access) Act 2025 ("**DUA Act**") was passed, which introduces a number of detailed changes to the UK GDPR and the UK Data Protection Act 2018

Summary and key findings

Annual aggregate fines remain broadly the same

For the year beginning 28 January 2025, European supervisory authorities issued fines totalling approximately EUR1.2bn (USD1.42bn/GBP1.06bn), broadly matching the previous year's figure. While there is no year-on-year increase in aggregate GDPR fines, this figure marks a reversal of last year's downward trend and underscores that European data protection supervisory authorities remain willing to impose substantial monetary penalties. Nine out of ten of the top ten individual fines imposed since 25 May 2018 have been imposed against big tech companies.

Country aggregate fines league table

Remaining in the top spot, with fines now totalling EUR 4.04bn (USD4.77bn/GBP3.56bn), the Irish DPC has issued eight of the top ten fines since 25 May 2018, including issuing a large fine this year of EUR530m (USD625m/GBP466m) against a social media company in relation to transfers of personal data to China.[7] France is now in second position with EUR1.1bn (USD1.3bn/GBP968m), however, in France, it is not always possible to separate fines imposed under the GDPR and those imposed under other regimes, such as e-privacy legislation,[8] therefore the aggregate value of fines issued under the GDPR in France may be inflated. Luxembourg is in third place this year, with fines totalling EUR746.56m (USD880.94m/GBP656.97), primarily due to the large fine of EUR746m (USD880m/GBP656m) imposed against a US online retailer and e-commerce platform in 2021. On 18 March 2025, the Administrative Court of Luxembourg dismissed the online retailer's appeal against the Luxembourg supervisory authority's ("**CNPD's**") fine and upheld the CNPD's initial decision.[9] The US online retailer and e-commerce platform is reportedly considering a further appeal. It is evident that large tech companies remain firmly in the sights of European data protection supervisory authorities, with no sign of relations thawing any time soon. The aggregate total fines reported since the application of GDPR on 25 May 2018 to 10 January 2026 across all the jurisdictions surveyed now stands at EUR7.1bn (USD8.4bn/GBP6.2bn).

Breach notifications increase

For the first time since 25 May 2018, average breach notifications per day have reached over 400 – breaking the plateauing trend we have seen in recent years. Between 28 January 2025 and 27 January 2026, the average number of breach notifications per day increased by 22% – from 363 to 443.[10] It is not clear what is driving this uptick in breach notifications, but the geo-political landscape driving more cyber-attacks, as well as the focus on cyber incidents in the media and the raft of new laws including incident notification requirements (e.g. under the Network and Information Security Directive[11] and the Digital Operation Resilience Act[12]), may be focusing minds on breach notifications. It is perhaps not surprising that the EU Digital Omnibus is proposing to raise the bar for incident notification to regulators, to capture only breaches which are likely to cause a high risk to the rights and freedoms of data subjects. Supervisory authorities have been inundated with notifications and understandably want to stem the flood so they can focus on the genuinely serious incidents.

Highest individual fine league table

#1

In May 2023, the Irish DPC imposed a record administrative fine of EUR1.20bn (USD1.42bn/GBP1.06bn) against Meta IE[13], as well as an order to suspend further transfers of EEA personal data 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.[14] In its decision, the Irish DPC concluded that Meta IE's reliance on the 2021 SCCs did not compensate for the deficiencies in US law identified in *Schrems II* – given that Meta IE cannot prevent surveillance of EU personal data by US public authorities with the SCCs and as there is no remedy for an EEA data subject who is not informed that they have been the subject of such surveillance. In addition, the Irish DPC concluded that Meta IE did not have any supplemental measures in place which would compensate for the inadequate protection provided by US law.

#2

Luxembourg's data protection supervisory authority, the CNPD, continues in the second position this year with a fine of EUR746m (USD880m/GPB656m) against a US online retailer and e-commerce platform. In March 2025, the Administrative Court of Luxembourg dismissed the online retailer's appeal against the CNPD's fine and upheld the CNPD's initial decision.[15]

#3

On 30 April 2025, the Irish DPC imposed a fine of EUR530m (US625m/GBP466m) against a social media company in relation to transfers of personal data to China.[16] The Irish DPC found that the social media company had infringed Article 46(1) GDPR by transferring personal data to a third country without ensuring and demonstrating that the personal data of EEA users subject to the transfers was afforded a level of protection essentially equivalent to that guaranteed within the European Union. As a result, the Irish DPC imposed an administrative fine of EUR530m (USD625m/GBP466m); an order mandating the company to bring its processing into compliance within six months; and an order suspending the company's transfers to China if it does not comply.

7 See: https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following

8 The aggregate fines data in this Survey includes fines imposed under Article 82 of the French Data Protection Act, by interpretation of Article 4(11) of the GDPR and therefore may include fines under other regimes, such as the e-privacy regime

9 Although the Court's decision is public, the national law on data protection obliges the CNPD to respect professional secrecy (Article 42) and prevents it from commenting on individual cases or publishing details of the decision

10 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

11 Directive (EU) 2022/2555 ("NIS2"). See: https://eur-lex.europa.eu/eli/dir/2022/2555

12 Regulation (EU) 2022/2554 ("DORA"). See: https://eur-lex.europa.eu/eli/reg/2022/2554

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

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

15 Although the Court's decision is public, the national law on data protection obliges the CNPD to respect professional secrecy (Article 42) and prevents it from commenting on individual cases or publishing details of the decision

16 See: https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following

Spotlight on GDPR compensation claims

There have been a number of significant decisions across the EU and UK relating to compensation claims. Some of these tend to favour claimants; others are better news for defendants. Some are more of a mixed bag.[17]

Europe's highest court, the CJEU, ruled in September 2025[18] following a referral from the German Federal Court of Justice (Bundesgerichtshof - "BGH") that non-material damage referred to in Article 82(1) GDPR can include negative feelings, such as fear or annoyance, provided the data subject can demonstrate that they are experiencing such feelings. This was a win for claimants. However, in the same decision, the CJEU ruled that the mere assertion of negative feelings is insufficient for compensation; national courts must assess evidence of such feelings and be satisfied that they arise from the breach of GDPR. This provides some comfort for defendants as theoretical distress is insufficient to sound in compensation.

In Ireland, the Supreme Court in *Dillon*[20] considered whether claims for non-material damage under the GDPR, such as emotional distress from a data breach, should be subject to the same procedures as personal injury claims. In *Dillon*, a personal data breach occurred when letters, containing Dillon's personal and financial information, were accidentally disclosed to a third party. Dillon brought Circuit Court proceedings, arguing that the data breach resulted from negligence and breach of statutory duty, and claiming damages for "*distress, upset, anxiety, inconvenience, loss and damage*".

Both the Circuit Court and, on appeal, the High Court, found that Dillon's claim amounted to seeking damages for personal injury, and consequently, required authorisation from the Injuries Resolution Board (formerly the Personal Injuries Assessment Board or PIAB) before the proceedings could be validly issued. Allowing Dillon's appeal, in a procedural win for claimants, the Supreme Court confirmed that such claims for non-material damage do not require authorisation from the PIAB. However, defendants can also take comfort from this decision which went on to say that the scope for obtaining significant compensation for these types of claims is "*very, very modest*".[21] Claimants seeking damages solely for distress or inconvenience, falling short of a psychiatric illness, should not expect more than very modest awards.

In the UK, the Court of Appeal held in *Equiniti*[22] that while it will still be necessary to establish that there was a breach of the GDPR, evidence of disclosure to a third party is not required for a viable claim – fear alone is sufficient, provided that the fear is objectively justified, which should be determined on a case-by-case basis. In this case, Equiniti mistakenly sent sensitive pension statements to outdated postal addresses. The error raised concerns that the data could be accessed by unauthorised individuals, prompting a group action against Equiniti under the GDPR and the UK Data Protection Act 2018. Prior to this case, English law required claims for compensation for non-material damage to meet a "*threshold of seriousness*" to proceed which was a useful deterrent to more spurious claims and therefore beneficial to defendants.

In *Equiniti*, the English Court of Appeal (considering existing case law from the CJEU which, although not legally binding in the UK post-Brexit, remains persuasive jurisprudence) effectively removed this obstacle by confirming that there is no "threshold of seriousness" for compensation claims for non-material damage. This is a win for claimants and could pave the way for more claims including group litigation claims. That said, defendants can still take comfort from the fact that claimants have to demonstrate that "*fear of an infringement*" is objectively justified rather than hypothetical or speculative.[23]

The law regarding claims for compensation for non-material damage is diverging as cases are decided by different domestic Member State courts. That said, some of the key open questions of law regarding what evidence is required to meet the relevant burden of proof for compensation for non-material damage have been tackled by the courts during 2025. As jurisprudence continues to evolve and remove legal uncertainty we anticipate that claimants, their lawyers, and in some jurisdictions their litigation funders, may be emboldened to bring more claims for compensation, including group claims. Organisations should therefore factor in the risk of compensation claims for breach of GDPR when assessing and managing compliance risk.

17 GDPR is an EU Regulation so applies directly in each Member State. The UK GDPR is for all intents and purposes the same as the EU GDPR as retained EU law post Brexit. That said, there is variation in interpretations across each different Member State and the UK. Coupled with this, there are procedural differences across different Member States and the UK which impact the risk of claims. In particular, some Member States (and the UK) have procedures facilitating group litigation which increases the risk and potential quantum and cost of defending claims for defendants. Some Member States permit litigation funding which can also compound the risk of compensation claims and group litigation. The picture and risk of claims (and the costs of defending them) is therefore mixed across the EU and UK

18 See: *IP v Quirin Privatbank AG C-655/23*

19 See: CJEU, judgment of October 4, *2024 – C-200/23*

20 See: *Dillon v Irish Life Assurance plc [2025] IESC 37*

21 See: paragraph 56, *Dillon v Irish Life Assurance plc* [2025] IESC 37

22 See: *Farley v Paymaster 1836 Ltd (trading as Equiniti)* [2025] EWCA Civ 1117

23 See: paragraphs 77 – 87 of : *Farley v Paymaster 1836 Ltd (trading as Equiniti)* [2025] EWCA Civ 1117

Spotlight on changes to the GDPR

In recent years the EU has introduced an extensive suite of regulations including the AI Act,[24] the Data Act,[25] NIS2, the CRA,[26] DORA, the DSA,[27] the DMA[28] and more under the 'Digital Decade' banner. These measures aim to safeguard fundamental rights, foster trust in technology, and create a level playing field. In practice, however, businesses and even governments often view Europe through a blurred regulatory lens: overlapping scopes of different laws and regulations, inconsistent definitions, multiple reporting channels, fragmented enforcement, and complex interactions between regimes.

Proposed changes to the EU GDPR

On 19 November 2025, the European Commission unveiled its proposed Digital Omnibus.[29] The initiative seeks to "*simplify, clarify and improve*" the existing Digital Decade package of laws and regulations, and includes amendments to the GDPR, as well as setting out amendments to the EU's broader digital regulatory framework.

Among others, the proposals include a single EU breach reporting portal and common template, which aims to address the duplicative reporting and administrative burden resulting from overlapping obligations for organisations under the GDPR, NIS2, DORA and other frameworks. Based on a "*report once, share many*" principle, the proposed amendments would: (i) raise the threshold for notifying data protection authorities to cover only breaches posing a high risk to individuals (a list of examples are to be provided by the EDPB); (ii) extend the reporting deadline for notifying supervisory authorities from 72 to 96 hours; and (iii) introduce a centralised portal operated by the EU agency for cybersecurity, ENISA, using a harmonised incident reporting form (to be provided by the EDPB), which would also address other overlapping notification requirements (e.g., under NIS2 / DORA).

The proposed data protection reforms aim to ease compliance burdens and introduce practical mechanisms – such as the single breach reporting portal – that could assist businesses in fulfilling compliance requirements. Some privacy advocates have been quick to criticise the proposals, describing them as a "*death by a thousand cuts*" and alleging a covert fast-track assault on the GDPR.[30] If simplification is perceived as undermining fundamental rights, the outcome could be legal uncertainty, increased litigation, and political backlash – the very opposite of the simplification and clarity businesses seek. The Omnibus therefore faces a delicate balancing act: simplifying rules without eroding trust or core rights. It is expected that the proposals will change as they are debated among the European Commission, the European Parliament, and the EU Council during the trialogue process in 2026.

Changes to the UK GDPR and UK data protection laws

In the UK, the Data (Use and Access) Act 2025 ("**DUA Act**")[31] was passed and received Royal Assent on 19 June 2025. The DUA Act introduces reforms to data protection and e-privacy laws. While the overall impact of the amendments to the UK's data protection framework are relatively modest, the DUA Act makes a large number of detailed changes to the UK GDPR and the Data Protection Act 2018. In particular, the DUA Act introduces the concept of 'recognised legitimate interests' to provide a presumption of legitimacy to certain processing activities that a controller may wish to carry out under Article 6(1)(f) UK GDPR (legitimate interests). One of the more significant areas of reform relates to Automated Decision Making ("**ADM**"). The amendments aim to promote innovation and use of AI systems and remove the requirement to establish a qualifying lawful basis before conducting ADM (the requirement currently at Article 22(2) UK GDPR), except where special category data is used. The amendments should help to ease the existing challenge where ADM is used in areas such as recruitment where the alternative legal bases of consent / contract necessity are problematic. The ICO has indicated that enforcement action may be prioritised where ADM systems lack transparency or fail to offer meaningful human intervention. The DUA Act also grants the Secretary of State the authority to designate new special categories of personal data and additional processing activities that fall under the prohibition of processing special category data in Article 9(1) of the UK GDPR.

In relation to transfers of personal data to third countries, the DUA Act introduces amendments that are designed to clarify the UK's approach to the transfer of personal data internationally and the UK's approach to adequacy assessments. The DUA Act introduces the data protection test, which replaces the test of essential equivalence (under the EU regime) with a new threshold that the third country offers safeguards that are "*not materially lower than*" the UK.

The UK Information Commissioner ("**ICO**") will also be re-constituted and given enhanced powers, including in relation to enforcement of ePrivacy breaches. The practical impact of these amendments is yet to be seen and the core GDPR principles remain intact. As the ICO revises and updates its guidance in the coming months, the impact of the changes, and the need to manage any divergence between the UK GDPR and EU GDPR will become clearer.

Although some of the DUA Act provisions came into force automatically, many of the DUA Act's provisions need to be commenced via secondary regulations. The government set out its plans to commence these provisions in stages,[32] with the majority of the data protection provisions expected to enter into force in the coming months (with the exception of those provisions that may require a longer lead-in time, such as the new complaints process).

24 Regulation (EU) 2024/1689 ("EU AI Act"). See: https://eur-lex.europa.eu/eli/reg/2024/1689

25 Regulation (EU) 2023/2854 ("Data Act"). See: https://eur-lex.europa.eu/eli/reg/2023/2854

26 Regulation (EU) 2024/2847 ("CRA"). See: https://eur-lex.europa.eu/eli/reg/2024/2847

27 Regulation (EU) 2022/2065 ("DSA"). See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

28 Regulation (EU) 2022/1925 ("DMA"). See: https://eur-lex.europa.eu/eli/reg/2022/1925

29 See: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

30 See for example: https://noyb.eu/en/digital-omnibus-first-analysis-select-gdpr-and-eprivacy-proposals-commission

31 See: https://www.legislation.gov.uk/ukpga/2025/18/contents

32 The Department for Science, Innovation and Technology has published a summary of the Government's plans for bringing into force provisions in the DUAA. See: https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement

Commentary

Enforcement trends

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

As predicted in last year's survey, European data protection supervisory authorities have continued to prioritise the importance of the lawfulness, fairness and transparency principle (Article 5(1)(a) GDPR), with failures to comply with this principle consistently remaining one of the top enforcement priorities for regulators. During its October 2025 plenary, the EDPB picked compliance with the obligations of transparency and information under the GDPR as the topic for its fifth coordinated enforcement action[33] and there have been a number of large fines during 2025 for breaches of this principle. For example, the Dutch Data Protection Authority ("**Dutch AP**") imposed a fine of EUR2.7m (USD3.2m/GBP2.4m) on a credit reference agency ("**CRA**") for various breaches of the GDPR including breach of the lawfulness, fairness and transparency principle.[34]

This fine from the Dutch AP came after the CRA filed an objection against the Dutch AP's initial decision and imposition of a fine in December 2023 (the value of the fine was not disclosed), for breaches of the GDPR, as well as two penalty orders requiring the CRA to remedy the violations. At the request of customers (such as telecom providers, online retailers, and landlords), the CRA prepared creditworthiness reports on individuals, collecting a large amount of data, such as negative payment behaviour, outstanding debts, or bankruptcies, from a variety of public and non-public sources, including the Trade Register of the Chamber of Commerce and telecom and energy companies that sell data from their customers. This enabled the CRA to create an extensive database containing personal data, including special category personal data, on a significant number of individuals within the Netherlands. The Dutch AP initiated an investigation following complaints from consumers who reported being asked to pay large deposits or being denied credit by service providers, without being informed that this was linked to credit scores issued by the CRA or that credit checks had been conducted.

Following its investigation, various breaches of the lawfulness, fairness and transparency principle were identified by the Dutch AP. In particular, the Dutch AP found that the CRA was in breach of the transparency principle by collecting data about consumers from a variety of both public and private sources without adequately informing individuals. The Dutch AP concluded that the CRA could not rely on the exemption to the right to be informed when obtaining personal data from a third party under Article 14(5) GDPR. The Dutch AP further found that the CRA did not have an adequate legal basis for processing personal data, In particular, the AP held that the CRA did not clearly show why processing certain personal data was strictly necessary – rather than just "nice to have" – for creditworthiness assessments and therefore could not rely on legitimate interest as a legal basis. In addition, the Dutch AP concluded that the CRA failed to adequately balance the interests of the individuals concerned – finding that individuals' rights outweighed the CRA's claimed legitimate interest.
The Dutch AP suggested that a key safeguard could have been a very short retention period tailored to this processing, but concluded that the CRA largely followed outdated industry guidelines with long retention periods that could not be considered adequate under current law and technology developments.

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. In the UK, the ICO imposed a fine of EUR16m (USD19m/GBP14m) on Capita for failing to ensure the security of personal data related to a breach in 2023 that resulted in hackers stealing millions of people's information.[35] The decision gives some indication of key areas where organisations should be taking proactive steps to reduce security risks. In particular, the Information Commissioner found that Capita had failed to implement appropriate technical and organisational measures to safeguard the data they held, in particular, the organisation had failed to prevent privilege escalation and unauthorised lateral movement, respond appropriately to security alerts or implement adequate penetration testing and risk assessment.

In Germany, the Federal Commissioner for Data Protection and Freedom of Information (**BfDI**) imposed a fine of EUR30m (USD35.4m/GBP26.4m) on a telecommunications service provider for breaches of Article 32(1) of the GDPR. This decision is of particular note as the BfDI launched an investigation into the service provider after receiving *"external communication without any complaints"* or any notified security breach.[36] The provider offered an online service portal for its customers. When used in combination with the company's hotline, the BfDI identified authentication vulnerabilities for the customer accounts, which had the potential to lead to misuse of eSIMs. The BfDI also imposed an additional fine of EUR15m (USD17.7m/GBP13.2m) for breaching Article 28(1) GDPR. The authority found deficiencies in the provider's data processing agreements, particularly around supervision and auditing of processors, as well as weaknesses in the processors' IT systems – creating a risk that customer data could be exploited for fraud.

There have also been some significant court decisions in Germany in relation to monitoring and auditing obligations of controllers with respect to their processors. In a decision on immaterial damages under Article 82 GDPR, the Higher Regional Court of Dresden addressed the monitoring and auditing measures that a controller must exercise over its processor and how these measures must be designed.[37] The case involved a data breach at a former processor of the controller. The contract between the controller and the processor had ended several years before the data breach at the end of 2019. According to the data processing agreement, the controller could choose between deletion or return of the data after the end of the processing. However, the controller never exercised this right. A few days before the termination of the agreement, the processor informed the controller by email that the data would be deleted the following day. Almost a year later, in December 2020, the processor sent another email to the controller announcing that the deletion was imminent. However, it was not until early 2023, and after the data breach had been reported, that the processor confirmed to the controller that deletion had been carried out.

In its judgment, the Court dealt extensively with the issue of a controller's liability for the omissions of its processor. In particular, the court found that if a company selects an IT service provider that is known in the market as a leading and reliable provider, it can generally place trust in the provider's expertise and reliability without the need for an on-site inspection, but increased requirements apply if large amounts of data or particularly sensitive data is hosted.
In the opinion of the Higher Regional Court, in the specific case this meant that the controller was obliged to exercise its rights towards the processor with respect to the deletion of the data and, in case of deletion, obtain written confirmation of the deletion. In addition, if necessary and deletion remains outstanding, the controller should carry out an on-site inspection. The court also clarified that mere announcements of the processor to delete the data (in the future) are not an adequate substitute for the confirmation that the data has already been deleted.

33 See: https://www.edpb.europa.eu/news/news/2025/coordinated-enforcement-framework-edpb-selects-topic-2026_en. In a coordinated action, the EDPB prioritises a certain topic for European data protection supervisory authorities to work on at national level. Participating European data protection supervisory authorities will join this new action on a voluntary basis and the action itself will be launched over the course of 2026

34 See: https://autoriteitpersoonsgegevens.nl/actueel/experian-krijgt-boete-van-27-miljoen-euro-voor-privacyovertredingen?trk=public_post_comment-text (in Dutch only)

35 See: https://ico.org.uk/action-weve-taken/enforcement/2025/10/capita-plc/

36 See: https://www.edpb.europa.eu/news/national-news/2025/german-federal-sa-administrative-fines-amount-eu15-000-000-and-eu30-000-000_en

37 Case number 4 U 940/24. See: https://openjur.de/u/2498248.html

Supply chain security and compliance is increasingly attracting the attention of EU data protection supervisory authorities. Supervisory authorities expect robust controls to prevent misuse and breaches and processors, as well as controllers, are directly liable for GDPR breaches. In March 2025, the UK ICO fined Advanced Computer Software Group Ltd ("**Advanced**") – an IT and software services provider - EUR3.49m (USD4.12m/GBP3.07m) for security failings.[38] Advanced processed personal data on behalf of its customers, which included the NHS and other healthcare providers. In 2022, hackers accessed certain systems of Advanced's health and care subsidiary via a customer account that did not have multi-factor authentication. The security incident led to disruption to critical services such as NHS 111, and other healthcare staff were unable to access patient records. The ICO found that Advanced's health and care subsidiary did not have the appropriate technical and organisational measures in place to keep its health and care systems fully secure. This marked the ICO's first fine against a processor under the UK GDPR and indicates the supervisory authority's recognition of the widespread impact of security failures by processors serving multiple controllers.

Transfers of personal data to third countries

Transfers of personal data to third countries outside of the EEA continue to attract regulatory attention. This year, the Irish DPC issued a fine of EUR530m (USD625m/GBP466m) against a social media company in relation to transfers of personal data to China.[39] The Irish DPC found that the social media company had infringed Article 46(1) GDPR by transferring personal data to a third country without ensuring and demonstrating that the personal data of EEA users subject to the transfers was afforded a level of protection essentially equivalent to that guaranteed within the EU. As a result, the Irish DPC issued an administrative fine of EUR530m (USD625m/GBP466m); an order mandating the company to bring its processing into compliance within six months; and an order suspending the company's transfers to China if it does not comply. The decision is the first that concerns remote access as opposed to data storage and highlights the importance of conducting a TIA – and as part of that assessing a third countries' data protection standards and identifying and implementing any additional measures to be taken - to ensure there is an essential equivalent level of protection.

However, there has been welcome news for some on EU-U.S. data transfers of personal data. In September 2025, the EU General Court dismissed French MEP, Philippe Latombe's, challenge to the EU-U.S. Data Privacy Framework ("**DPF**") for the transfer of personal data between the EU and U.S.[40] Less than two months after the EU-U.S. adequacy decision was adopted, Latombe submitted challenges[41] to the European Union General Court demanding the immediate suspension of the EU Commission's adequacy decision and challenging the legality of the DPF. Latombe argued that: under the DPF, U.S. intelligence agencies can still access large amounts of EU citizens' data, in violation of the GDPR's principles of data minimisation and proportionality; the DPF's Data Protection Review Court ("**DPRC**") is not an independent tribunal and does not offer guarantees similar to those required by Article 47 of the Charter of Fundamental Rights and Article 45(2) of the GDPR; and the DPF does not address the absence of safeguards in the U.S. around ADM and data security.

The General Court dismissed Latombe's action for annulment, finding, in particular that the appointment of judges to the DPRC and the DPRC's functioning are "*accompanied by sufficient safeguards and conditions to ensure the independence of its members*". In particular, the Court referred to the fact that judges of the DPRC may only be dismissed by the Attorney General and only for cause, and the Attorney General and intelligence agencies must not unduly impede or influence the work of the DPRC. The Court also noted that the judgment in *Schrems II* does not suggest that the bulk collection of personal data must be subject to prior authorisation issued by an independent authority; rather that *Schrems II* instead requires that the decision authorising such collection must, at the very least, be subject to judicial review. The Court found that signals intelligence activities carried out by U.S. intelligence agencies, including when they carry out bulk collection of personal data, are subject to the subsequent judicial supervision of the DPRC, whose decisions are final and binding. Therefore, the bulk collection of personal data carried out by the intelligence agencies satisfies the requirements arising from the judgment in *Schrems II*. The Court rejected Latombe's argument in relation to the absence of safeguards equivalent to those in the EU relating to ADM and security. In particular, the Court held that sectoral protections provided for by U.S. law must be taken into account and that the judgments in both *Schrems I* and *Schrems II* do not require a third country to guarantee a level of protection identical to that guaranteed in the EU.

The General Court made it very clear that its decision was based on the facts and law as they stood at the time when the European Commission's adequacy determination was adopted (10 July 2023). Accordingly, the Court did not address potentially relevant developments under the Trump administration including the firing of, and not replacing, members of Privacy and Civil Liberties Oversight Board (currently before U.S. Courts) and multiple alleged violations of U.S. privacy laws by U.S. government agencies.

The General Court's decision marked a significant moment in the ongoing saga of EU-U.S. data transfers. While the General Court's decision was welcomed by organisations transferring personal data from the EU to the U.S., the debate is far from settled and the decision provides only temporary legal certainty. Latombe has already brought an appeal against the General Court's decision[42] and the ruling is limited to the specific challenges raised by Mr. Latombe and does not preclude future legal challenges based on different arguments, circumstances or new facts arising since July 2023. Whilst the General Court cites the *Schrems II* decision, there is a notable shift in the way the Court ascribes a more general approach to assessing essential equivalence, as compared to the existing rigour provided in the European Essential Guarantees set forth by the EDPB. In addition, the European Commission will continuously monitor the adequacy decision and DPF and may suspend or amend the decision.

38 See: https://ico.org.uk/media2/gdlfddgc/advanced-penalty-notice-20250327.pdf

39 See: https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following

40 See: https://curia.europa.eu/juris/documents.jsf?num=T-553/23

41 See: https://curia.europa.eu/juris/document/document.jsf?text=&docid=279601&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=15723212

42 See: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202506610]

Looking back at our predictions for 2025

In last year's report, we predicted that:

- the "consent or pay" model would remain in the regulatory cross-hairs;
- there would be a continued focus on the personal liability of company officers and directors and other individual members of management bodies for infringements of GDPR as a lever to drive better compliance;
- data protection supervisory authorities and organisations developing, deploying and using AI would continue to grapple with the relationship between AI and data protection law;
- European data protection supervisory authorities would continue to prioritise the importance of the lawfulness, fairness and transparency principle (Article 5(1)(a) GDPR); and
- the UK would continue to take a "less is best" approach to enforcement.

Consent or pay model

The "consent or pay" model has remained a hot topic of discussion among European data protection supervisory authorities and privacy activists. This year, the Austrian Federal Administrative Court ("**BVwG**") examined the legality of "consent or pay" models. The case focused on the approach adopted by the Austrian daily newspaper *DerStandard.at*, which gave users a choice between paying a subscription fee or consenting to extensive data processing for advertising purposes. The BVwG ruled that the consent obtained by the newspaper under the "consent or pay" model was invalid. The court specifically criticised the mechanism for obtaining consent, which it held unlawfully bundled separate processing purposes, preventing users from giving selective consent and breaching the principle of granularity required under data protection law. According to the BVwG, users were placed under undue pressure by the binary "*all-or-nothing*" choice and consequently provided consent that did not reflect their genuine intent. As evidence of this coercive effect, the court referred to the near-total consent rate observed on the newspaper's website. Against this backdrop, the BVwG held that the consent obtained under the "consent or pay" model could not be considered as freely given, and therefore failed to meet the criteria for valid consent within the meaning of Art. 4(11) GDPR. The BVwG's decision aligns with the EDPB opinion adopted in April 2024,[43] which, although not closing the door on consent or pay models, sets a very high bar for such models to be lawful. However, it remains to be seen if European data protection supervisory authorities will follow suit. In the UK, the Information Commissioner has taken a more pragmatic approach and welcomed Meta's decision to shift its advertising model to a 'consent or pay' model, stating that the low starting price point for UK users (close to half that for EU users) provides UK consumers with a fair choice between consenting to targeted ads using their data or paying to subscribe with no ads.[44]

Personal liability

There has been a continued focus on the personal liability of management bodies and individuals. Notably, in October 2025, following the Dutch DPA's statement last year that it intended to investigate whether the directors of Clearview AI could be held personally responsible for the company's ongoing violations of GDPR,[45] the privacy activist group, NOYB, announced that it had filed a criminal complaint in Austria against Clearview AI Inc. and its managers under the GDPR and the Austrian Data Protection Act ("**DSG**").[46] Clearview AI has faced a raft of penalties from European data protection supervisory authorities,[47] after a series of complaints dating back to May 2021 by privacy activists and other digital rights organisations. In Austria, the Austrian Data Protection Authority ("**DSB**") held in 2023 that Clearview AI's collection and use of facial images and related data violated the GDPR. The DSB ordered the deletion of the data but did not impose a general ban or issue a fine. NOYB's criminal complaint against Clearview AI signals an upping of the ante from administrative enforcement to potential criminal liability for individual members of Clearview AI's management team. Given that Clearview AI has no EU presence, enforcement of sanctions remains a challenge.

AI

As predicted, data protection supervisory authorities and organisations developing, deploying and using AI have continued to grapple with the relationship between AI and data protection law. Enforcement action during 2025 included a fine of EUR5m (USD5.9m/GBP4.4m) imposed by the Italian data protection supervisory authority ("**Garante**") against Luka Inc. in relation to its Replika service, a chatbot with a written and voice interface based on a generative AI system.[48] The Garante found that Luka Inc. was in breach of Articles 5.1 (a) and 6; Articles 5.1 (a), 12, 13, 5.1 (c), 24 and 25.1 of the GDPR, by failing to identify the legal basis for the data processing operations carried out through Replika and failing to provide an adequate fair processing notice. The Garante also found that Luka Inc. had not implemented any age verification mechanisms – either at registration or during use of the service – despite having declared that minors were excluded from potential users.

While enforcement action by EU data protection supervisory authorities has continued, regulators are increasingly under pressure to strike a balance between robust data protection rights and fostering innovation – making the EU a more attractive destination for innovators in the public and private sectors. For example, the Irish DPC announced that it has been actively engaging with many big tech companies in relation to AI developments, in particular concerning the use of adults' personal data to train large language models in the EU/EEA.[49] In 2024, Meta informed the Irish DPC of its plans to train its large language model using public content shared by adults on Facebook and Instagram across the EU/EEA. The Irish DPC engaged with both Meta and the EDPB and made a number of recommendations regarding the potential impact on the data protection rights of individuals. The Irish DPC has stated that these recommendations have led to Meta implementing a number of significant measures and improvements regarding the processing taking place.

The Digital Omnibus proposals[50] also aim to provide greater clarity regarding the balance between data protection rights and the use of AI. The proposed amendments to the GDPR include a broad set of AI-related exceptions – including introducing GDPR exceptions for AI development and operations under the 'legitimate interest' basis, subject to safeguards such as data minimisation, transparency, and a right to object; and an exemption under Article 9(2) GDPR, allowing residual processing of special category personal data when developing and deploying AI systems, subject to certain safeguards. While this would be a welcome clarification regarding the appropriate lawful basis for AI, critics caution that although these safeguards may apply during training, the term 'operations' could encompass any personal data processing, making it difficult to rely on legitimate interest consistently. The proposal also creates a limited exemption for sensitive data inadvertently present in AI datasets, allowing retention under protective measures when removal would require disproportionate effort.

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

44 See: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/09/ico-statement-on-changes-to-meta-advertising-model/

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

46 See: https://noyb.eu/en/criminal-complaint-against-facial-recognition-company-clearview-ai

47 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)

48 See: https://gpdp.it/home/docweb/-/docweb-display/docweb/10132048

49 See: https://www.dataprotection.ie/en/news-media/latest-news/dpc-statement-meta-ai

50 See: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

Lawfulness, fairness and transparency principle

In last year's survey we predicted that European data protection supervisory authorities would continue to prioritise the importance of the lawfulness, fairness and transparency principle (Article 5(1)(a) GDPR). As set out above, failures to comply with the principle have continued as one of the top enforcement priorities for regulators, with the EDPB choosing compliance with the obligations of transparency and information under the GDPR as the topic for its fifth coordinated enforcement action.[51] This year we have seen a continuation of multiple and significant fines issued by data protection supervisory authorities for breach of this core principle, including a fine of EUR6.4m (USD7.6m/GBP5.6m) imposed by the Polish data protection supervisory authority against the Minister of Digital Affairs for processing the data of 30 million citizens without a valid legal basis;[52] and a fine of EUR2.7m (USD3.2m/GBP2.4m) imposed by the Dutch AP against a credit reference agency for various breaches of the GDPR, including breach of the transparency principle.

UK Information Commissioner

Finally, we predicted last year that the UK's ICO would continue to take a "less is best" approach to enforcement. With the notable exception of several fines imposed during 2025 for breach of the GDPR security principle, which remains a key enforcement priority for data protection supervisory authorities in all jurisdictions surveyed, enforcement has otherwise continued to be limited in the UK relative to the EU. The lack of ICO enforcement triggered an open letter in November 2025 from over seventy civil liberties groups, academics and privacy advocates which urged the Chair of the Select Committee for Science Information and Technology to open an inquiry "*into the collapse in enforcement activity by the Information Commissioner's Office*".[53] The letter states that there is a broad trend "*which has seen the ICO shying away from using its enforcement powers*" and "*other instances where the ICO issued reprimands or significantly lowered the awarded fines*". The letter concludes by urging the committee to open an inquiry "*to investigate the Information Commissioner's Office, and understand why data protection enforcement appears to be a low priority*". With cyber-attacks recognised as representing an existential threat to the UK's national security and economic stability,[54] a clear exception to the ICO's less is best approach is continued enforcement of the GDPR security principle. In October 2025, the ICO imposed a fine of EUR16m (USD19m/GBP14m) on Capita for failing to ensure the security of personal data related to a significant and widely reported breach in 2023.[55] Further, in December 2025, the ICO fined password manager provider LastPass UK Ltd EUR1.4m (USD1.7m/GBP1.2m) following a 2022 data breach that compromised the personal information of up to 1.6 million of its UK users. The ICO found that LastPass had failed to implement sufficiently robust technical and security measures, which led to unauthorised access to its backup database, although there was no evidence that hackers were able to unencrypt customer passwords as these are stored locally on customer devices and not by LastPass.

51 See: https://www.edpb.europa.eu/news/news/2025/coordinated-enforcement-framework-edpb-selects-topic-2026_en. In a coordinated action, the EDPB prioritises a certain topic for European data protection supervisory authorities to work on at national level. Participating European data protection supervisory authorities will join this new action on a voluntary basis and the action itself will be launched over the course of 2026

52 See: https://uodo.gov.pl/pl/138/3590

53 See: https://www.openrightsgroup.org/press-releases/70-organisations-and-experts-demand-action-over-failing-ico/

54 See: https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyber-attacks-on-the-uk/summary-of-research-on-the-economic-impact-of-cyber-attacks

55 See: https://ico.org.uk/action-weve-taken/enforcement/2025/10/capita-plc/

Predictions for the year ahead

Our predictions for the year ahead include:

Continued focus on the GDPR security principle

We predict there will be an increased focus on enforcement of the GDPR security principle in the year ahead, including more investigations and enforcement action against suppliers acting as processors for multiple different customer controllers. This trend will be driven by heightened geopolitical tensions and damaging cyber-attacks which pose an existential threat to the resilience of financial services, utilities and other essential and important services underpinning our societies. One-to-many suppliers are attractive targets to threat actors as they are often a repository for sensitive information relating to multiple different customers and can also be a gateway to customer networks and digital assets. The trend will also be driven by an increased legislative focus on the vital importance of supply chain security and resilience; for example, many of the regulations forming part of the EU's Digital Decade package such as NIS2, DORA, and the CRA contain mandatory supply chain security and resilience measures.

Focus on governance and accountability

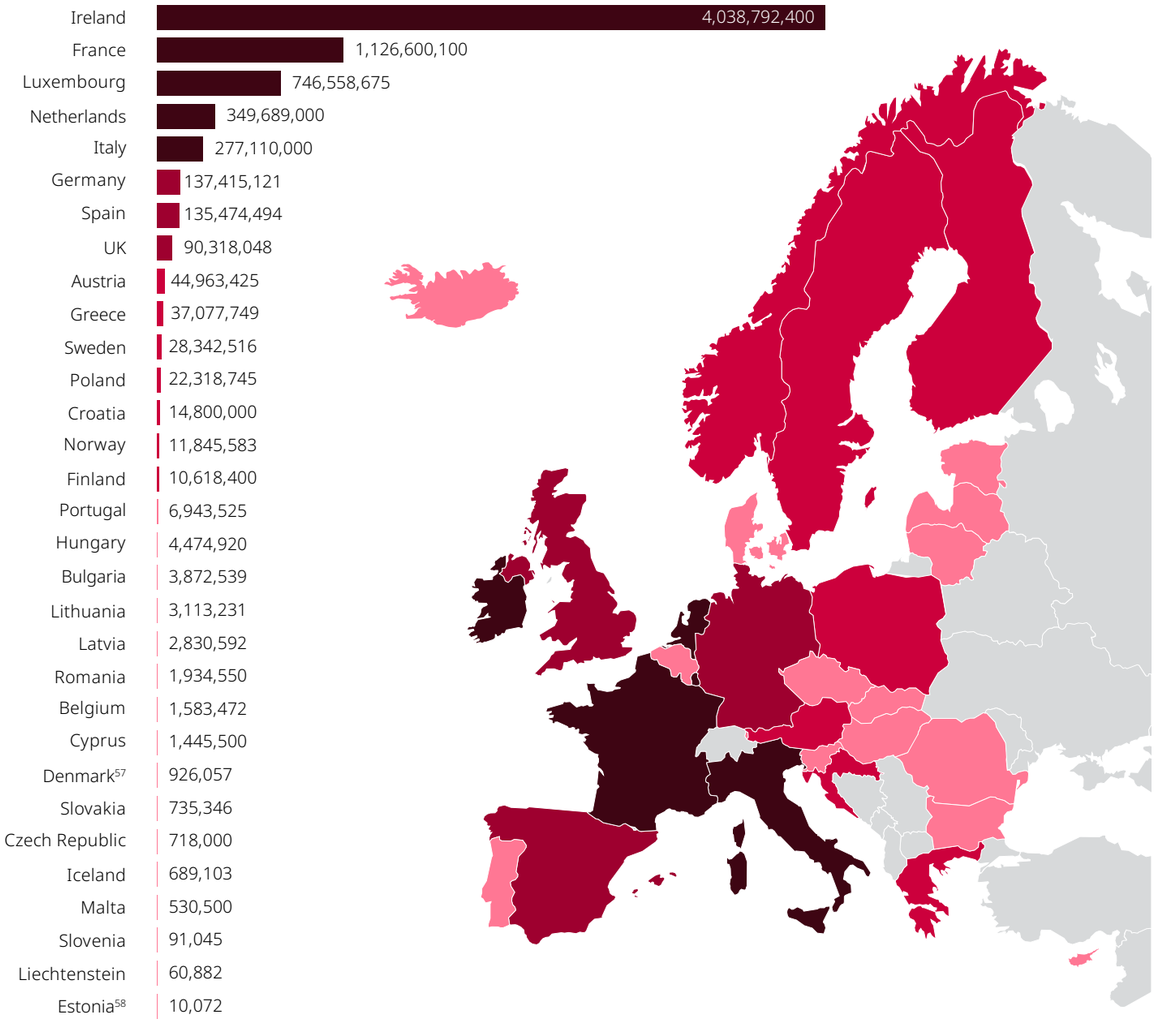
We predict that data protection supervisory authorities will place greater emphasis on the accountability principle and in particular ensuring Data Protection Impact Assessments ("DPIAs") are effective, taking into consideration all risks arising from high risk processing and regularly reviewed on an ongoing basis. During 2025, we have seen supervisory authorities criticise the lack of effective DPIAs and DPIA governance and refer to them as a core element of effective data protection risk management and governance. We anticipate that failure to prepare and oversee appropriate DPIAs for high risk processing activities will be an enforcement priority for regulators and will be cited as an aggravating factor when sanctions are imposed.

Continuing trends for enforcement

We predict that some of the trends we identified in last year's predictions will continue to remain a regulatory enforcement priority for the year ahead. Notably: the consent or pay model; the balance between AI innovation and data protection compliance; international personal data transfers; and the pre-eminence of the GDPR lawfulness, fairness and transparency principle will all remain enforcement priorities for the coming year.

Report

Total value of GDPR fines imposed from 25 May 2018 to date (in euros)[56]

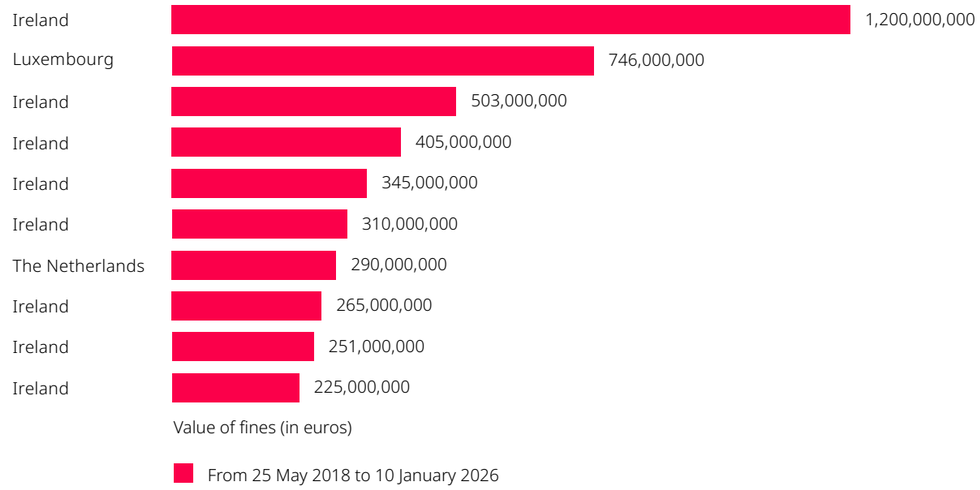


56 This report does not include fines that have been successfully appealed. In some jurisdictions, not all information in relation to fines is made publically available (such as in relation to Germany) or only part of the data for the period of this report has been provided (e.g. Bulgaria). Therefore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

57 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

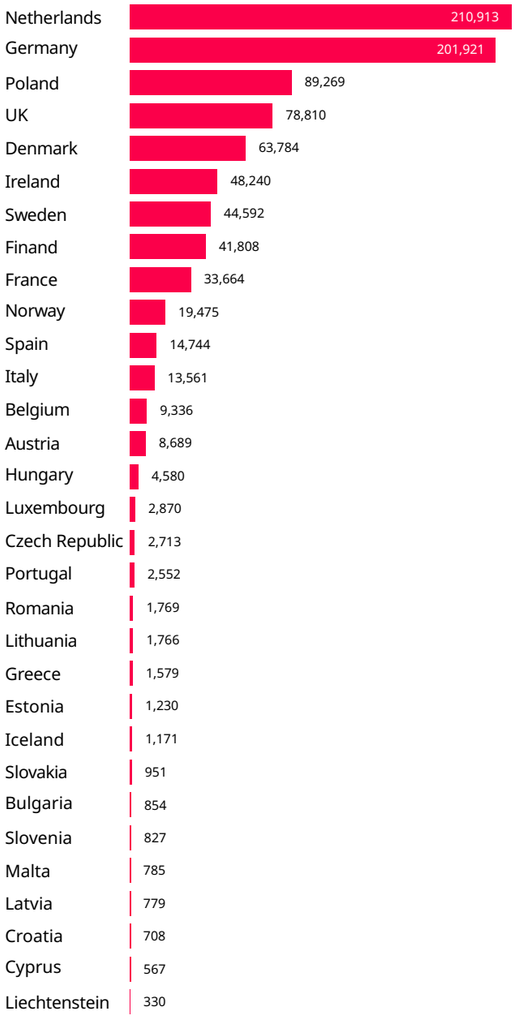
58 In Estonia, a fine of EUR3m (US3.5m/GBP2.6m), the largest fine issued to date by the Estonian Data Protection Authority, has not been included within this survey as the fine has not yet been enforced and is currently under appeal

Top largest fines imposed to date under GDPR[59]

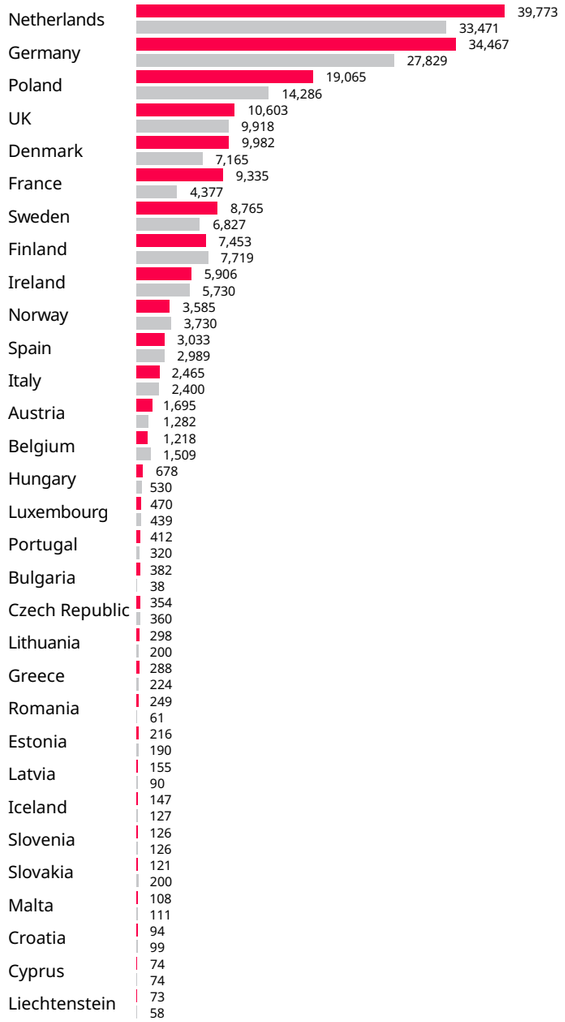


59 With respect to the top largest fines imposed to date under the GDPR, we have only included fines imposed under the GDPR (so for example it does not include fines imposed under other regimes such as e-privacy legislation)

Total number of personal data breach notifications between 25 May 2018 and 27 January 2026 inclusive*

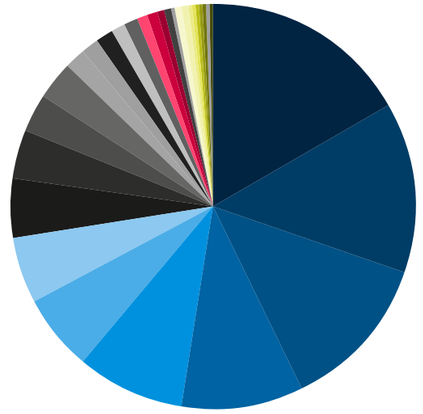


Total number of personal data breach notifications between 28 January 2025 and 27 January 2026 inclusive (last 12 month period)



* 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 2025 and 27 January 2026 (last 12 month period)	Change compared to last year's ranking*
Netherlands	223.79	No change
Lichtenstein	182.47	No change
Denmark	167.12	+1
Finland	132.46	-1
Ireland	112.86	No change
Sweden	82.77	+2
Luxembourg	70.04	No change
Norway	65.07	-2
Poland	49.27	No change
Germany	40.97	+1
Iceland	40.47	-1
Malta	23.03	No change
Austria	18.9	+2
Estonia	18.12	-1
UK	15.49	-1
France	13.65	+2
Lithuania	11.33	No change
Belgium	10.17	-2
Latvia	8.61	+4
Hungary	6.88	+2
Spain	6.42	+2
Slovenia	6	-2
Bulgaria	5.63	+7
Cyprus	5.59	-3
Italy	4.04	-1
Portugal	4.04	+1
Czech Republic	3.54	-1
Greece	2.75	+1
Croatia	2.27	-1
Slovakia	2.18	-5
Romania	1.37	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 2025 in a number of jurisdictions including Germany, the Netherlands, Belgium, Italy (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 200 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 250 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 AI Laws of the World

Our online AI Laws of the World handbook provides an overview of AI laws and proposed regulations across 40+ countries. It highlights key legislative developments, including regulations, proposed bills and guidelines issued by governmental bodies. The guide provides an insightful overview of AI developments, as well as some of the common thematic approaches of lawmakers and AI-focused organisations around the world.

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.

For access to all DLA Piper resources please visit: dlapiperintelligence.com.

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