

GDPR Fines & Data Breach Survey - Ireland levied over half of Europe's GDPR fines in 2024



Author: John Magee, Partner and Global Co-Chair of Data Protection, Privacy and Cybersecurity at DLA Piper and Member of Compliance Institute's Data Protection & Information Security Working Group.¹

Summary and Key Findings from DLA Piper 2025 Report:

Global law firm DLA Piper's latest General Data Protection Regulation (GDPR) Fines and Data Breach Survey shows that 2024 has been another busy period for enforcement with an aggregate total of EUR1.26bn of GDPR fines. While this represents a 33% decrease from the EUR 1.78 billion issued in the previous year, the decline is largely attributed to the absence of a record-breaking fine on the scale of Meta's EUR 1.2 billion penalty from the Irish DPC in 2023. The report offers insights gathered from all 27 EU Member States plus the UK, Norway, Iceland, and Liechtenstein. 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.

Big tech companies and social media giants remain the primary targets by regulators. However, European data protection supervisory authorities have demonstrated growing confidence and assertiveness during 2024 and are increasingly issuing fines in other sectors.

With the rapid adoption of artificial intelligence, the European regulators have signalled a more assertive approach to enforcement to ensure that AI training, deployment and use remains within the guard rails of the GDPR.

Continued trend of sizable fines

In recent years, data protection authorities have issued numerous fines amounting to hundreds of millions of Euros. In 2024, they have shown increased confidence and willingness to impose high fines. The Irish DPC has had another busy year, issuing a fine of EUR310m against LinkedIn in October 2024,² and a fine of EUR251m against Meta in December 2024.³ In August 2024, the Dutch DPA issued a fine

of EUR290m against a well-known ride-hailing app. In contrast the UK Information Commissioner John Edwards was quoted saying he does not believe the approach of high volume of fines to have the greatest impact.⁴ This is certainly an outlier approach compared with the rest of Europe and has been criticised by privacy activists.

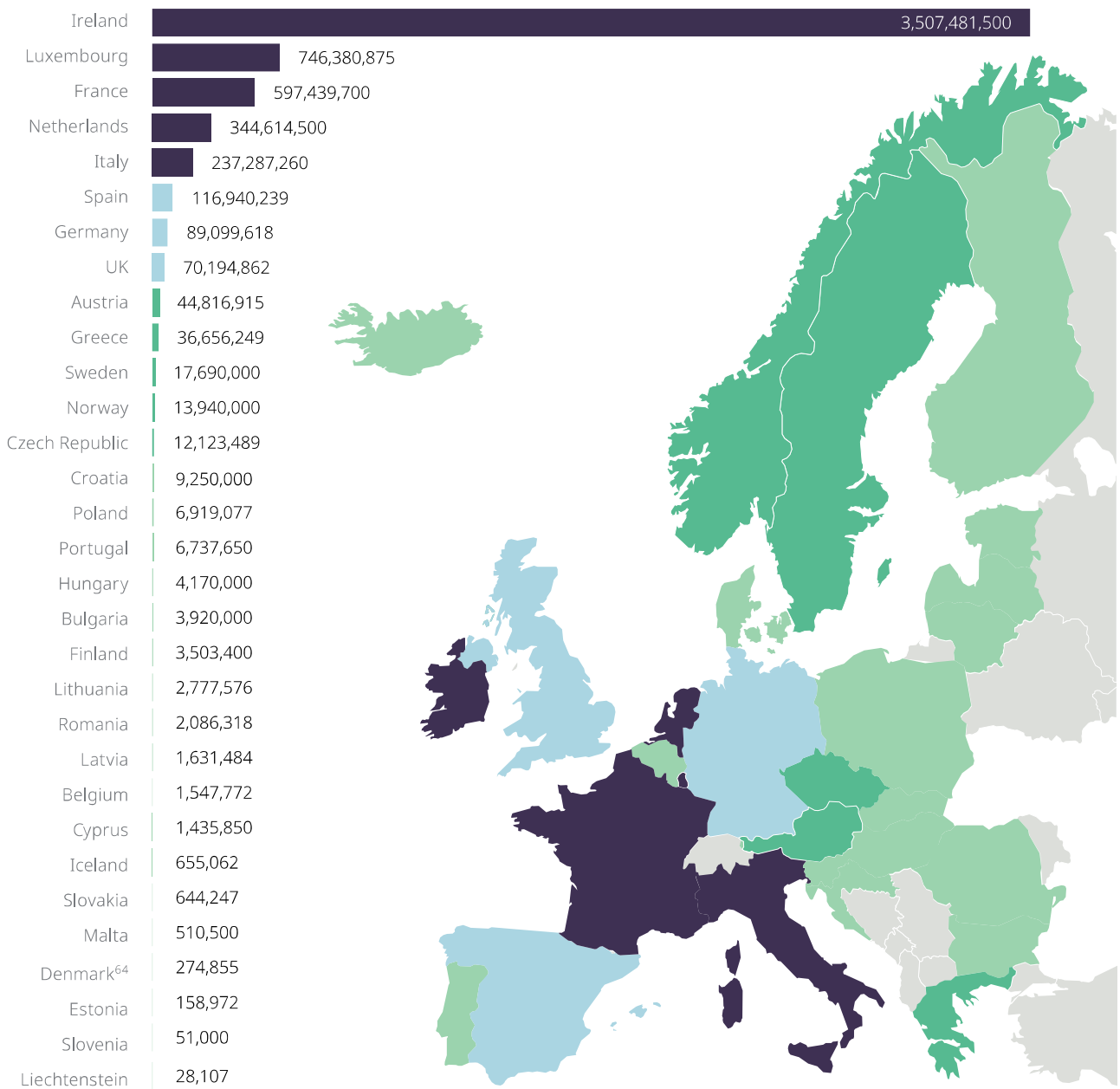
As with previous years, there is a continued trend of the biggest fines being imposed against big tech and social media giants; with nine out of ten of the top ten individual fines being imposed against organisations in this sector. However, other sectors are not out of the reach of regulators, with jurisdictions such as Italy and Spain issuing a high volume of fines across a variety of sectors, including two fines totalling EUR6.2m issued against a large bank by the Spanish Data Protection Authority,⁵ and EUR5m fine against an Italian utility provider for using outdated or inaccurate customer data to execute unsolicited electricity and gas contracts.⁶

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.⁷ 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. The Netherlands, Germany,⁸ and Poland remain in the top three spots for the highest number of data breaches notified in 2024, with Ireland coming in eighth place and fifth place on a per capita basis.

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.



Spotlight on personal liability and AI

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, they fined Clearview AI EUR 30.5 million.⁹ Clearview AI had collected facial images and data from the internet and social media without informing individuals, creating a global facial recognition database. This led to complaints from privacy activists and digital rights organizations since May 2021, resulting in multiple fines from various data protection authorities for GDPR violations. As Clearview AI has faced a raft of GDPR penalties over the last few years¹⁰ but continues to operate in the same way, the Dutch DPA also ordered incremental penalties of up to EUR5.1m.

In Ireland, the DPC issued suspension proceedings against X under Section 134 of the Data Protection Act 2018 which allows the 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. The High Court noting when they did, that this was the first time that any Lead Supervisory Authority had taken such an action. The order considered the processing of certain personal data for the purpose of training its AI chatbot tool, Grok, as data sharing was automatically turned on for users in the EU with no option to opt out.

Enforcement trends

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. For example, the Irish DPC fined LinkedIn. The inquiry focused on LinkedIn's use of personal data for behavioural analysis and targeted advertising. It examined data from LinkedIn members and third-party partners. Specifically, LinkedIn's consents for processing third-party data were deemed invalid as they were not freely given, sufficiently informed, specific, or unambiguous. Similarly, the Czech DPA fined Avast Software approximately EUR 14 million. The investigation revealed that Avast's branch, Jumpshot, Inc., had transmitted pseudonymized internet browsing history of around 100 million users to marketers. Users were misinformed about the data transfer, which was not anonymized, allowing for re-identification. The data was used not just for statistical analysis, but also for tracking online consumer behaviour without a lawful basis.

Cookies and similar tracking technologies

Earlier this year, the Court of Justice of the European Union (CJEU) ruled on a case involving Mr. Schrems and Meta (Facebook). Mr. Schrems argued that Meta unlawfully processed his personal data, including information about his sexuality, to

send him personalized ads without his consent or a lawful basis under the GDPR.¹¹ The CJEU decided that GDPR Article 5(1)(c) does not permit social network platforms to process data for personalized advertising indefinitely and without distinguishing the type of data. The court emphasized that data minimization requires limiting the retention period of personal data to what is strictly necessary for the processing purpose.

Last year, the European Data Protection Board (EDPB) held a consultation on draft guidelines regarding the scope of Article 5(3) of the e-Privacy Directive, known as the "cookie rule."¹² In October 2024, the EDPB adopted the updated guidelines.¹³ 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. However, these guidelines are not legally binding, and it will be up to the courts to determine if the EDPB has overstepped in its interpretation.

Predictions for the year ahead

Consent or pay model

The "consent or pay" model will remain in the regulatory cross-hairs during 2025. The EDPB¹⁴ and decisions by the Irish DPC¹⁵ have effectively closed the door to relying on other 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.¹⁶

Personal liability for officers and directors

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 Clearview 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.

AI enforcement

As the much-anticipated EDPB opinion on AI models¹⁷ does not provide many clear or definitive answers, 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 AI¹⁸ makes a clash of regulatory approaches more likely.

Focus on lawfulness, fairness and transparency

Finally, the European data protection supervisory authorities - including the DPC in Ireland - will continue to prioritise the importance of the lawfulness, fairness and transparency principle (Article 5(1)(a) GDPR).



REFERENCES

1. The author would like to thank and acknowledge the support of Laoise Murray in preparing this article.
2. See: <https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linked-in-ireland-eu310-million>
3. See: <https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million>
4. 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
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://www.garantepriacy.it/home/docweb/-/docweb-display/docweb/10053275#1>
7. 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.
8. 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.
9. See: <https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition>
10. Including from the Italian supervisory authority (see: <https://www.garantepriacy.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)
11. See: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0446>
12. See: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en
13. See: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf
14. See: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en
15. 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>.
16. See: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202404865.
17. See: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en
18. See: <https://www.presidency.ucsb.edu/documents/2024-republican-party-platform>