GDPR Fines & Data Breach Survey: Ireland Leads Europe with Record-Breaking Fines

Author: John Magee, Partner and Head of Data Protection, Privacy and Cybersecurity for Ireland at DLA Piper and member of Compliance Institute's Data Protection & Information Security Working Group.

Summary and Key Findings from DLA Piper 2024 Report:

Global law firm DLA Piper's latest General Data Protection Regulation (GDPR) Fines and Data Breach Survey shows that 2023 continued to see increasingly high GDPR fines with the value of GDPR fines imposed in Ireland now EUR2.86bn. The report offers insights gathered from all 27 EU Member States plus the UK, Norway, Iceland, and Liechtenstein. As Ireland remains a popular location for technology and other data rich companies to set up their main establishment in the EU, it is not surprising that it has rocketed to the top spot of the country league table for the aggregate value of fines imposed since May 2018. Ireland also takes the top spot for the largest fine ever imposed, with the EUR1.20bn fine issued against Meta by the Irish Data Protection Commission in May 2023.

Data driven social media and big tech remain the primary target for record fines across the countries surveyed with each of the top ten largest fines issued since 25 May 2018 being imposed on businesses in this sector.

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

Rise in value of aggregate fines imposed:

The aggregate total fines reported since the application of GDPR up to 8 January 2024 stands at EUR 4.68bn. The European data protection supervisory authorities have issued a total of EUR1.78bn in fines since 28 January 2023, representing an increase of 14.10% on the total of EUR1.56bn issued in the year from 28 January 2022. This level of increase is significantly less than the 50% increase reported last year, mainly due to a number of successful appeals in various jurisdictions, which have seen fines reduced or in some cases overturned. During 2023 there were also fewer fines issued by European data protection authorities following opinions and binding decisions of the European Data Protection Board ("EDPB") under the GDPR consistency mechanism.

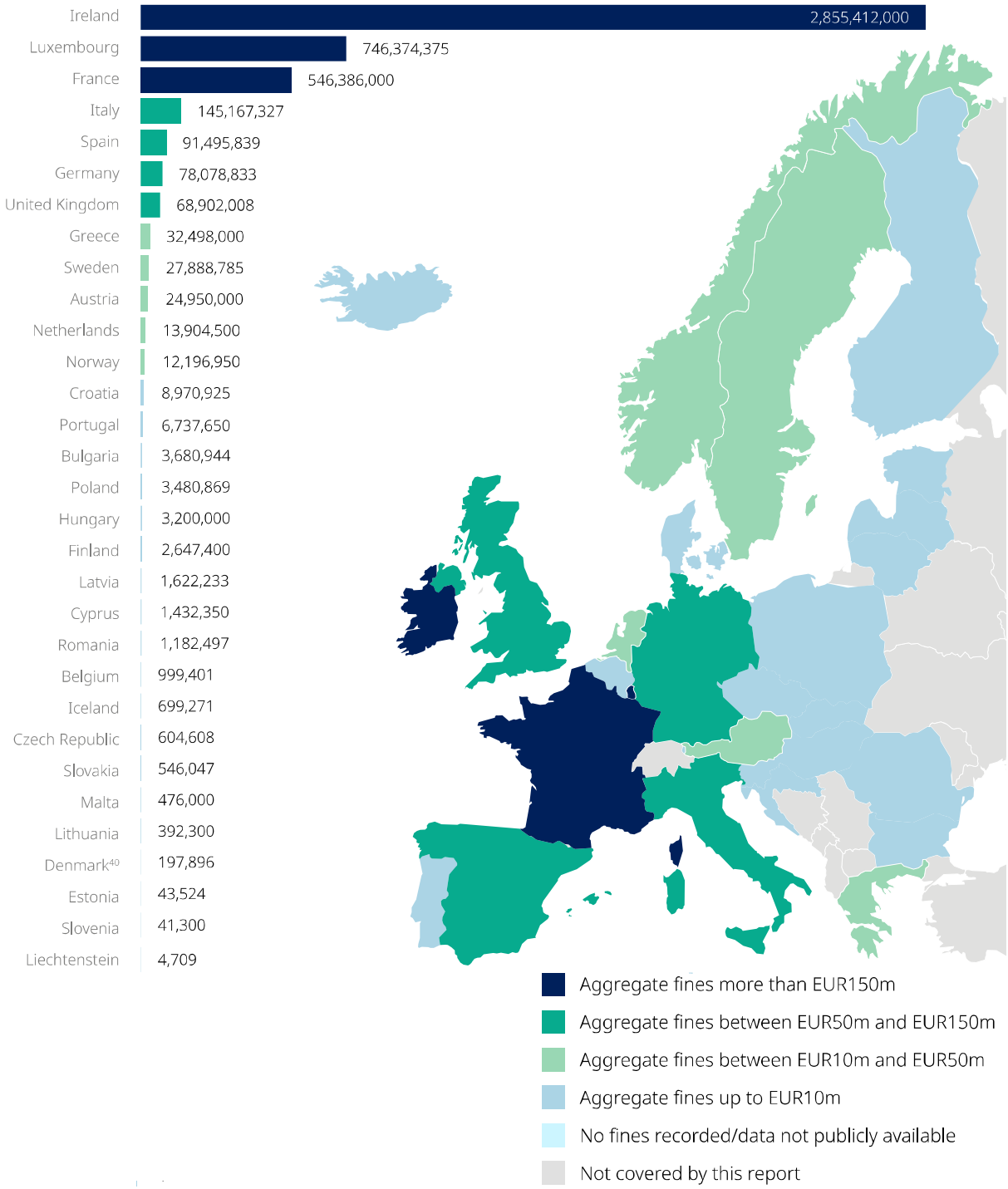
Country aggregate fines league table:

There is no change at the top of this year's country league table for the aggregate fines imposed to date since 25 May 2018. Ireland and Luxembourg remain in the top two spots, with fines totalling EUR2.86bn and EUR746m respectively. Given Ireland's popularity as a European headquarters for data driven social media and big tech businesses and the fact that the Irish Data Protection Commission is therefore frequently the lead supervisory authority for all cross-border processing throughout the EU, Ireland is likely to continue to be at the top of the table for years to come.

Breach notifications:

Conversely, there is effectively no year-on-year change in the overall number of breach notifications made, with 335 notifications made per day from 28 January 2023 to 27 January 2024 compared to 328 during the same period in 2022. The notification threshold remains open to interpretation and with the consequences of notifying a breach now more apparent with multiple fines issued for

Report



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

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

data breaches coupled with follow-on litigation and compensation claims, organisations which may initially have erred on notification may now be shying away from doing so. Germany and the Netherlands have reported the highest number of data breaches notified from 28 January 2023 to 27 January 2024, with 32,030 and 20,235 respectively. Ireland is sitting at 6th place with 6,912 data breaches notified in the same period.

Enforcement trends:

Failure to comply with the core GDPR principles continues to be the most frequently cited justification for fines across the jurisdictions surveyed and of all the principles set out in Article 5 GDPR, failures to comply with the lawfulness, fairness, and transparency principle (Article 5(1)(a) GDPR) remain the top enforcement priority.

Similarly, both supervisory authorities and courts are continuing to set a high bar for compliance with the requirement to demonstrate a lawful basis to process personal data. The "grand bargain" at the heart of the free internet has allowed social media and big tech to fund progressive consumer services by monetising data they collect on users of those services. However, this grand bargain is under attack and was the subject of the very largest fines reported in last year's survey. Significantly, on 27 October 2023, the EDPB adopted an urgent binding decision instructing the Irish Data Protection Commission to take final measures regarding Meta IE and to impose a ban on the processing of personal data for behavioural advertising on the legal bases of contract and legitimate interest across the entire EEA.

Spotlight on security of processing personal data:

Fines resulting from breaches of Article 5(1)(f) - the integrity and confidentiality principle - and the related Article 32 - security of processing - continue to feature across all jurisdictions surveyed. For example, in September 2023, the Irish Data Protection Commission announced a fine of EUR345m against a social media provider for non-compliance with GDPR rules regarding the processing of personal data of child users. What constitutes appropriate security measures meeting the standard required by Articles 5(1)(f) and Article 32 GDPR is likely to continue to be a key battle ground between regulators and the regulated in the years ahead. A failure to have appropriate governance and oversight over information security is one of the most cited aggravating factors by European data protection supervisory authorities when justifying penalties for security failures.

Spotlight on transfers:

Transfers of personal data to third countries outside of the EEA are still grabbing the headlines, with the highest fine to date of EUR1.20bn issued by the Irish Data Protection Commission for breach of Article 46(1) GDPR. Meta IE has commenced both an appeal

and judicial review of the decision through the Irish courts as well as an appeal against the EDPB's decision in the case through the EU courts.

Predictions for the year ahead:

DLA Piper's international Data, Privacy and Cybersecurity team provide an insight into what is expected in 2024. There will likely be more regulatory enforcement, appeals and litigation relating to the "grand bargain" while there will also likely be more bumps in the road for data transfers and the EU-US adequacy decision. As highlighted in last year's survey, transfers will continue to be a legal and compliance minefield for so long as the conflict of laws between GDPR and European Charter rights on the one hand and third country surveillance and interception laws on the other, remains.

Given the current inconsistencies among organisations in obtaining consent for cookies, fuelled by the practical challenges of obtaining consent significantly more complaints, investigations, and enforcement activity this year in relation to cookies and similar tracking technologies are anticipated.

With the explosion of new AI technologies continuing this year, continued investigations and enforcement into the more invasive and personal data rich AI systems and solutions are also expected.

European data protection supervisory authorities are also likely to continue to prioritise the importance of governance and oversight, with more enforcement where governance is found wanting. With the raft of new EU data and cyber legislation expected to come into force during 2024 and 2025, governance frameworks, including actionable steps to help govern data and cyber risks at all levels of an organisation and independent assurance that control frameworks are effective, will be increasingly important for organisations both to be able to comply with specific requirements for effective governance frameworks and to satisfy the accountability principle in Article 5(2) GDPR.

Finally, and closer to home, Dr Des Hogan and Dale Sunderland have been announced as the two new Data Protection Commissioners, succeeding the outgoing commissioner, Helen Dixon after 10 years as Europe's - and possibly the world's - most influential data protection regulator. This transition marks a significant milestone in Ireland's data protection landscape, signalling both continuity and greater breadth in leadership in the face of evolving regulatory challenge.

Dr Des Hogan and Dale Sunderland, Data Protection Commissioners.