DLA Piper GDPR Fines and Data Breach Survey

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:

Global law firm DLA Piper's latest annual General Data Protection Regulation (GDPR) Fines and Data Breach Survey shows that 2022 was another record year with an aggregate of €1.64bn GDPR fines reported across Europe, 50% more than the value of fines reported in 2021. Ireland's Data Protection Commission has taken its place at the top of the league table for aggregate fines imposed to date.

Ad-tech and behavioural advertising were a key enforcement priority this year, with the Irish Data Protection Commission issuing penalties of EUR210m against Facebook and EUR180m against Instagram in relation to their profiling practices.

Where fines were referred to and decided by the European Data Protection Board (EDPB) under the GDPR consistency mechanism during 2022, there was on average a 630% increase required by the EDPB compared to the fine originally proposed by the lead supervisory authority.

Country Aggregate Fines:

Ireland is now at the top of this year's country league table for the aggregate fines imposed to date, with fines now totalling over EUR1.3bn. Luxembourg is in second position, with the highest individual fine of EUR746m imposed in 2021. As Ireland and Luxembourg are popular locations for technology companies to establish in the European Union and as all the highest fines in these jurisdictions were imposed on technology companies under the GDPR's lead supervisory authority - "one-stop shop" - enforcement mechanism, it is perhaps not surprising that Ireland and Luxembourg remain in the top spots this year.

Decrease in Data Breach Notifications:

The increase in data breach notifications we have seen in recent years has started to level off. The average number of breach notifications per day from 28 January 2022 to 27 January 2023, was 300 compared to 328 during the same period last year. A total of approximately 109,000 personal data breaches were notified to regulators since 28 January 2022, a small decrease on last year's total of approximately 120,000. The reduction in breach notifications may be indicative of organisations becoming more proficient of reporting data breaches given the risk of investigations, enforcement, fines and compensation claims that may follow notification.

Focus on Artificial Intelligence (AI) Enforcement:

There has also been a notable increase in focus by supervisory authorities on the use of Artificial Intelligence (AI) technologies, with several high fines imposed on Clearview AI Inc for violations of the principles of lawfulness and transparency. Since many AI systems will use personal data at some point during their lifecycle, regulation of these systems often falls within the scope of GDPR. Several data protection supervisory authorities have issued guidance on the use of personal data for AI this year.

European data protection supervisory authorities recognise the link between AI systems and personal data. And given the European Commission's new laws and proposed legislation as part of its digitalisation strategy, there is an increasing risk that certain processing activities, including those in relation to the use of AI systems, will fall within the scope of both the GDPR and other European legislation - each with different enforcement rules and competent authorities. There is a potential for organisations to face investigations and enforcement actions from multiple supervisory authorities arising from the same use of artificial intelligence.

International transfers of personal data:

The decision of Europe's highest court in the case commonly referred to as Schrems II has created significant legal uncertainty and challenges for data exporters across the EEA, requiring highly complex assessments of the laws and practices of third countries and risk assessments. Compounding this challenge, the legal standard to be applied to personal data transfers from the EEA to third countries has been the subject of recent regulatory and judicial attention.

There have been some notable decisions made by data protection supervisory authorities considering the application of the Schrems II and Chapter V GDPR requirements to specific transfers, including the DPC's record €1.2bn fine and transfer suspension order issued against Meta in May 2023.

Enhanced Safeguards for transatlantic data transfers:

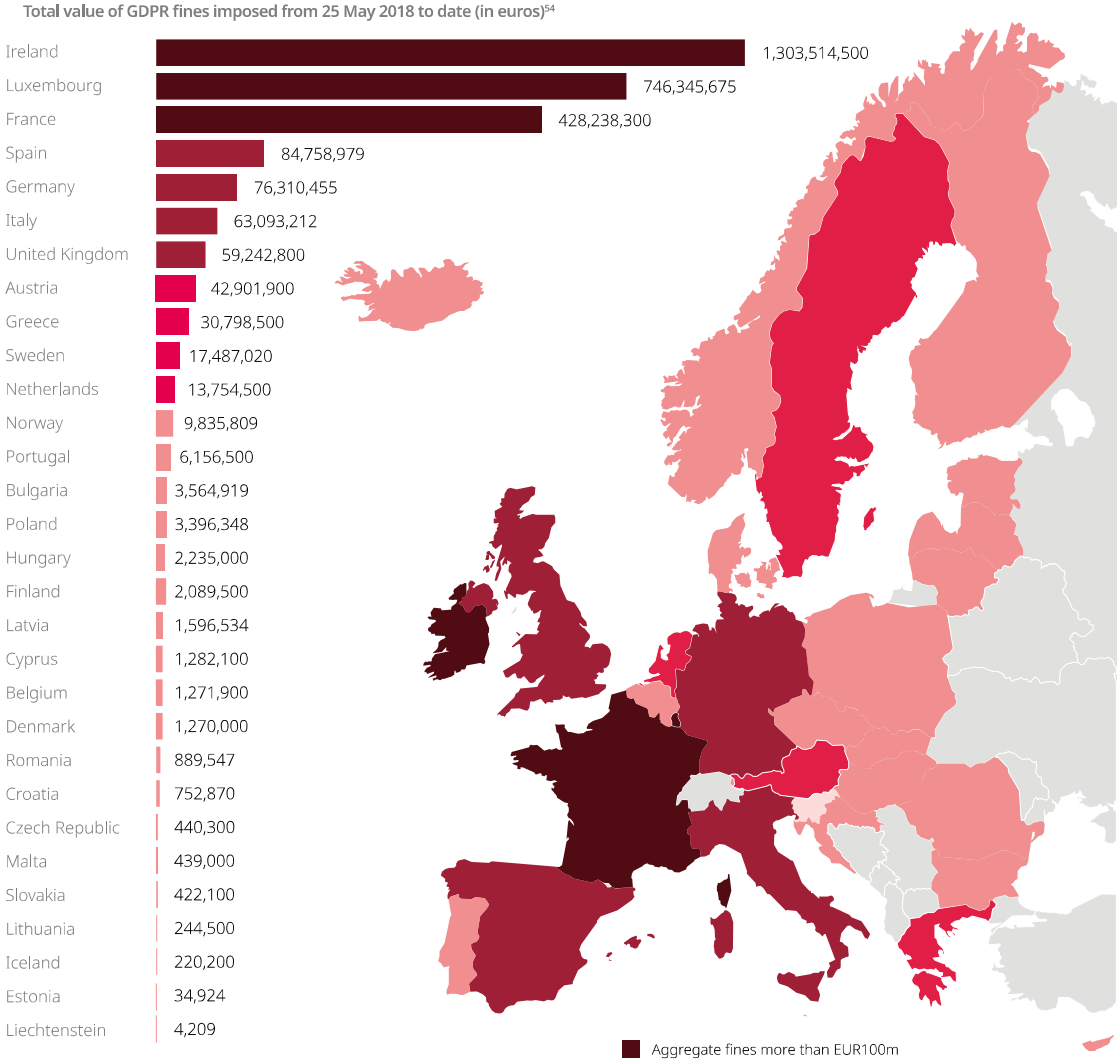
On 7 October 2022, President Biden issued an Executive Order to enhance Safeguards for United States Signals Intelligence Activities, which aims to address the legal uncertainty that has prevailed with respect to transatlantic data transfers since the Schrems II decision. Following last spring's joint U.S.-EU announcement of a "deal in principle" on an enhanced EU-U.S. Privacy Shield Framework, the EO directs U.S. intelligence agencies to take steps to implement U.S. commitments under the renamed EU-U.S. Data Privacy Framework.

SCHREMS III?

The long-term durability of any new U.S. adequacy decision remains unclear. While EU Commissioners and U.S. officials are confident the new adequacy decision will address the concerns with U.S. law raised in Schrems II, such a decision is all but certain to find its way back to the Court of Justice of the European Union for review based on a variety of alleged shortcomings. In addition, notwithstanding significant political and industry backing on both sides of the Atlantic, a final adequacy decision on the DPF is by no means guaranteed. Under the EU's comitology procedure, the EDPB has issued a non-binding (but nevertheless influential) opinion on the draft adequacy decision, and a "qualified majority" of at least 55 percent of the EU Member States must then approve the draft.

Report

Total value of GDPR fines imposed from 25 May 2018 to date (in euros)[54]



54 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 and Lithuania) or only part of the data for the period of this report has been provided (e.g. Bulgaria and Croatia). Therefore the real figure is likely to be higher than reported.