A REPORT BY DLA PIPER'S CYBERSECURITY AND DATA PROTECTION TEAM

DLA Piper GDPR fines and data breach survey: January 2023

DLA PIPER

DLA Piper GDPR fines and data breach survey: January 2023

2022 was another record year with an aggregate of EUR1.64bn (USD1.74bn/ GBP1.43bn) GDPR fines reported across Europe.[1] The aggregate value of fines issued in 2022 was 50% more than the value of fines reported in 2021.

As predicted in last year's survey, ad-tech and behavioural advertising were a top enforcement priority this year. The Meta group were on the receiving end of some of the very largest fines with the Irish Data Protection Commission issuing penalties of EUR210m (USD223m/GBP183m) against Facebook and EUR180m (USD191m/ GBP157m) against Instagram in relation to their profiling practices.[2]

At the heart of the internet is a grand bargain between online service providers and consumers: social media, search and other innovative services are offered "for free" in exchange for the consumer's personal data which is then monetised by enabling brands to serve personalised adverts to the consumer online. The recent decisions against Facebook and Instagram attack the cornerstone of this grand bargain and raise the question how will online services be paid for if online service providers cannot harvest and monetise consumer data? Allowing online service providers to harvest personal data has become a prerequisite to fund the innovation and development of many progressive technologies that have (in large part) benefited society. What these decisions highlight is just how important the "grand bargain" is to make the online ecosystem work. As that ecosystem has evolved and become more complex there has arguably been a breakdown in the understanding of the grand bargain between consumers and online service providers. A reset is urgently required to restore trust, greater transparency and to preserve the many benefits of the online ecosystem. With so much at stake and as the law in this area remains very far from settled, appeals are inevitable.

1 This survey covers all 27 Member States of the European Union, plus the UK, Norway, Iceland and Liechtenstein. Not all jurisdictions publish details of fines issued. It is possible that more fines have been issued and not published. We have reported on fines published during the period covered by this survey. Some fines were issued several weeks or months before publication. The UK left the EU on 31 January 2020. The UK has implemented GDPR into law in each of the jurisdictions within the UK (England, Northern Ireland, Scotland and Wales). As at the date of this survey the UK GDPR is the same in all material respects as the EU GDPR. That said, the UK Government Department for Digital, Media, Culture and Sport recently consulted on proposed changes to UK data protection laws "Data: a new direction" and is proposing to legislate changes to UK data protection laws during the course of 2023. It remains to be seen the extent to which these changes will deviate from the EU GDPR.

2 See: https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland. Meta IE has announced its intention to appeal both the substance of the decisions and the fines imposed thereunder.

"The recent decisions against Facebook and Instagram attack the cornerstone of the grand bargain between online service providers and consumers; they raise the question how will online services be paid for if online service providers cannot harvest and monetise consumer data? A reset is urgently required to restore trust, greater transparency and to preserve the many benefits of the online ecosystem."

The inflationary influence of the influential EDPB was also evident this year. Where fines were referred to and decided by the 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.[3]

The authors of this survey would like to thank the many different contributors and supervisory authorities who make it possible.[4]

3 This calculation is based on the following EDPB decisions: Binding Decision 2/2022 on the dispute arising on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) (the DPC proposed a fine of between EUR202m - EUR405m and issued a final fine of EUR405m): https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22022-dispute-arisen_en.; Decision 01/2022 on the dispute arising on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR (the CNIL proposed a fine of EUR100,000 and issued a final fine of EUR600,000: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/decision-012022-dispute-arisen-draft_en; and Binding decisions regarding Facebook, Instagram and WhatsApp (DPC proposed a fine of between EUR28m and EUR36m and issued a final fine of EUR390m (at the time of publication we are awaiting the full decision of the DPC and EDPB. The DPC claims in its press release that it proposed "very substantial fines" on Meta in relation to these breaches, which is understood to have been between EUR28m and EUR36m)): https://edpb.europa.eu/news/news/2022/edpb-adopts-art-65-dispute-resolution-binding-decisions-regarding-facebook-instagram_en. In some of these references, the lead supervisory authority proposed a range of fines. Where this was the case, the percentage increase calculation is based on the percentage increase between the lowest fine proposed and the actual fine set by the EDPB.

4 This survey has been prepared by DLA Piper UK LLP. 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.

Summary and key findings

Fines continuing to increase

The fine[5] of EUR746m (USD790m/GBP649m)[6] imposed by the Luxembourg data protection supervisory authority in July 2021 still remains the highest individual fine issued to date.[7] However, the Irish Data Protection Commissioner ("**DPC**") has imposed a number of record-breaking fines this year on Meta IE[8] including a fine of EUR405m (USD429m/GBP352m)[9] relating to the processing of children's personal data and a fine of EUR265m (USD281m/GBP231m)[10] relating to compliance with the GDPR obligation for Data Protection by Design and Default (both currently under appeal). The DPC started 2023 with two huge fines against Facebook and Instagram of EUR210m (USD223m/GBP183m) and EUR180m (USD191m/GBP157m)[11] respectively, relating to their consumer profiling practices used for behavioral advertising. The aggregate total fines reported since the application of GDPR on 25 May 2018 to 10 January 2023 now stands at EUR2.92bn (USD3.10bn/GBP2.54bn).

50% year on year increase in reported fines

This year supervisory authorities across Europe have reported a total of approximately EUR1.64bn (USD1.74bn/GBP1.43bn) in fines since 28 January 2022, which is an increase of 50% compared to the total of EUR1.09bn (USD1.16bn/GBP0.98bn)) issued in the year from 28 January 2021. The increase demonstrates supervisory authorities' growing confidence and willingness to impose high fines for breaches of the GDPR, particularly against large technology vendors; and has also been influenced by the highly inflationary impact of the EDPB. Local data protection authorities will no doubt have been watching the EDPB decisions under the GDPR consistency mechanism with interest and will know that the EDPB is yet to reduce any fine proposed by a lead supervisory authority. All EDPB decisions regarding fines have resulted in a significant increase in the final fine imposed.

There has also been a notable increase in focus by supervisory authorities on the use of Artificial Intelligence, with a number of high fines imposed on Clearview AI Inc for violations of the principles of lawfulness and transparency.[12]

5 All references in this survey to infringements or breaches of GDPR and to fines imposed are to findings made by relevant data protection supervisory authorities. In a number of cases, the entity subject to the fine has disputed these findings and the findings and penalties imposed are subject to ongoing appeal procedures. DLA Piper makes no representation as to the validity or accuracy of the findings made by relevant supervisory authorities.

6 In this report we have used the following exchange rates: EUR 1 = USD 1.06/GBP 0.87.

7 See: DLA Piper GDPR fines and data breach survey: January 2022.

8 This survey includes fines up to and including 10 January 2022.

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

10 See: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry.

11 See: https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland.

12 See Italy: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323; UK: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/; Greece: https://www.homodigitalis.gr/wp-content/uploads/2022/07/HellenicDPA_ClearviewDecision_13.7.2022_.pdf and France: https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet. The Australian Information Commissioner and Privacy Commissioner also found that Clearview AI, Inc. breached Australians' privacy by scraping their biometric information from the web and disclosing it through a facial recognition tool, however, this is outside the scope of this report.

Country aggregate fines league table

Ireland is now at the top of this year's country league table for the aggregate fines imposed to date, with fines now totaling over EUR1.3bn (USD1.38bn/GBP1.13bn). Luxembourg is now in second position, with the highest individual fine of EUR746m (USD790m/GPB649m) imposed in 2021. As Ireland and Luxembourg are popular locations for technology companies to establish in the European Union and as all of the highest fines in these jurisdictions were imposed on technology companies, it is perhaps not surprising that Ireland and Luxembourg remain in the top spots this year. We anticipate that this trend is likely to continue with tech companies still very much in the cross hairs of European data protection supervisory authorities and no apparent thawing of relations on the horizon.

Decrease in annual 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, is 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.[13] This decrease may be in part due to the fact that organisation's GDPR notification procedures have become more mature and also due to more sophisticated recording of data breach notification figures by data protection supervisory authorities. The reduction in breach notification may also be indicative of organisations becoming more wary of reporting data breaches given the risk of investigations, enforcement, fines and compensation claims that may follow notification.

13 Not all the countries covered by this report make breach notification statistics publicly available and many 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. 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 2021, some figures in last year's report that were previously extrapolated have been updated in this report.

Highest individual fine league table

#1

Luxembourg – EUR746m

Luxembourg's data protection supervisory authority, the CNPD, maintains the top position this year with a fine of EUR746m (USD790m/GBP649m) against a US online retailer and e-commerce platform issued in 2021. The fine is not publicly available and is still subject to an ongoing appeal.

#2

Ireland – EUR405m

On 2 September 2022, the DPC imposed a record EUR405m (USD429m/GBP352m) fine on Meta IE (in relation to Instagram) which is the largest fine to date issued by the DPC. This is the first EU-wide decision on children's data protection rights and highlights the special protection merited with regards to the processing of children's personal data. The DPC's Draft Decision was referred to the EDPB under Article 65 of the GDPR (Dispute resolution by the Board) for a binding decision. The EDPB found that there had been an infringement of Article 6(1) GDPR and instructed the DPC to consider the additional infringement in its compliance order. As a result the DPC imposed the maximum fine of the range it originally proposed to the EDPB for consideration of EUR405m (USD429m/GBP352m).[14]

#3

Ireland – EUR265m

The third highest fine since the application of GDPR on 25 May 2018, was again issued by the DPC. The DPC issued a fine of EUR265m (USD281m/GBP231m) against Meta IE, data controller of the "Facebook" social media network.[15] The material issues in the DPC's inquiry concerned questions of compliance with the GDPR obligation for data protection by design and default. The DPC held that Meta IE had failed to implement adequate technical and organisational measures pursuant to Article 25 GDPR.

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

15 See: https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry.

Spotlight on Enforcement concerning Artificial Intelligence

Artificial intelligence is impacting every sector, from process automation, machine learning, chat bots, facial recognition through to virtual reality and beyond. Personal data is often the fuel that powers AI used by organisations. It tailors search parameters, spots behavioural trends, and predicts future possible outcomes (to highlight just a few uses). 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. The European Data Protection Board issued guidance on specific areas of AI processing (most recently for the use of facial recognition technology in law enforcement).[16] In addition, several data protection supervisory authorities have issued detailed toolkits and opinions on the lawful use of AI systems for processing personal data (for example, the UK,[17] Dutch,[18] Italian[19] and Spanish[20] supervisory authorities).

As with data transfers, privacy activists are also focussing on processing of personal data by artificial intelligence and machine learning. Notably, Max Schrems through his organisation My Privacy is None of Your Business ("**noyb**") along with other digital rights organisations, filed legal complaints to data protection supervisory authorities in France, Austria, Italy, Greece and the United Kingdom against the facial recognition company Clearview AI Inc ("**Clearview AI**"), resulting in multiple investigations and several fines and enforcement actions.

BACKGROUND TO AI ENFORCEMENT ACTIVITY

Clearview AI collected images of people's faces and data from publicly available information on the internet and social media platforms around the world and provided an online global database that could be used for facial recognition, allowing its customers to check images against all the images in the database. Individuals were not informed that their personal data was used in this way and the database contained a substantial amount of data. Following a series of complaints filed in May 2021 by noyb and other digital rights organisations, several data protection supervisory authorities issued monetary penalties against Clearview AI for breaches of the GDPR.

On 9 March 2022, the Italian supervisory authority ("**Garante**"),[21] issued a monetary penalty of EUR20m (USD21.2m/EUR17.4m) against Clearview AI finding that the company infringed several fundamental principles of the GDPR. Similarly, on 23 May 2022, the UK Information Commissioner's Office ("**ICO**") fined Clearview AI GBP7.6m (USD9.2m/EUR8.6m) for breaches of the UK GDPR (currently under appeal).[22] This was followed by similar fines from the Greek data protection supervisory authority ("**HDPA**")[23] and the French supervisory authority ("**CNIL**"),[24] both issuing maximum fines of EUR20m (USD21.2m/EUR17.4m) against Clearview AI.

16 See: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

17 See: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-artificial-intelligence-and-data-protection/.

18 See: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/ai-algoritmes.

19 See: https://www.garanteprivacy.it/temi/intelligenza-artificiale.

20 See: https://www.aepd.es/es/documento/requisitos-auditorias-tratamientos-incluyan-ia-en.pdf.

21 See: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323.

22 See: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.

23 See: https://www.homodigitalis.gr/wp-content/uploads/2022/07/HellenicDPA_ClearviewDecision_13.7.2022_.pdf.

24 See: https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai.

In addition to this, in previous years (2020 and 2021), data protection supervisory authorities in Sweden,[25] Finland[26] and the Hamburg Commissioner issued decisions against Clearview AI and users of Clearview AI's services. The willingness of data protection supervisory authorities to enforce directly against users of artificial intelligence rather than just targeting Clearview AI as the provider of the technology is notable and a cautionary tale for organisations knowingly or unknowingly using AI across their supply chains.

The risk of double jeopardy

There is a growing trend among European data protection supervisory authorities to openly grapple with AI issues, recognising the inextricable link between AI systems and personal data. This looks likely to continue. In addition, given the European Commission's raft of new laws and proposed legislation as part of its digitalisation strategy,[27] 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. This risk will be compounded by the many new laws, proposed laws and guidance relating to artificial intelligence around the world, particularly those with extra-territorial application.

In addition, fines have been issued against Clearview AI across multiple European countries all relating to the same AI solution – demonstrating the risk of double and indeed multiple jeopardy. The fines are also an illustration that for non-EU based organisations, there is a risk that the same processing will trigger multiple enforcement action and fines across every market they target in the EEA and the UK. The theory was that the risk of multiple enforcement action could be mitigated by establishing a main establishment for cross-border processing within the EEA and selecting a "friendly" jurisdiction for that purpose. The effectiveness of that tactic is debatable in light of the increasingly hawkish and active EDPB and the ability of DPAs in other Member States to invoke the cooperation and consistency mechanism in the GDPR where they object to a draft decision by a different supervisory authority.[28]

25 In February 2021, the Swedish (IMY) fined the Swedish Police Authority for unlawfully processing biometric data for facial recognition through the use of services provided by Clearview AI and for failing to conduct a DPIA in breach of the GDPR. See: https://www.imy.se/en/news/police-unlawfully-used-facial-recognition-app/.

26 The Finish DPA found that the Finish National Police Board had unlawfully processed biometric data through a trial use of Clearview AI's automated facial recognition technology. The DPA ordered the National Police Board to notify a data breach to data subjects whose identity was known and to request Clearview AI to remove police-transmitted data from its systems. See: https://tietosuoja.fi/-/poliisille-huomautus-henkilotietojen-lainvastaisesta-kasittelysta-kasvojentunnistusohjelmalla.

27 In particular, the European Commission has published the long-awaited proposal for a Regulation on Artificial Intelligence which introduces a first-of-its-kind, comprehensive, harmonized, regulatory framework for Artificial Intelligence. See: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

28 Article 60(4) and 65(1)(a) GDPR.

Spotlight on international transfers of personal data and enforcement of Schrems II

The decision of Europe's highest court in the case commonly referred to as *Schrems II*[29] 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.[30] 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. Following complaints from noyb,[31] several Member State data protection supervisory authorities opened investigations into how exporters are complying with international data transfer restrictions. This year, we have seen several formal decisions in relation to these investigations - with European data protection supervisory authorities adopting an absolutist interpretation of the GDPR[32] in the context of data transfers under Article 46 GDPR.[33]

CASES AND ENFORCEMENT ACTIVITY

There have been some notable decisions made by data protection supervisory authorities this year considering the application of the *Schrems II* and Chapter V GDPR requirements to specific transfers. These include:

- The Austrian supervisory authority ("**DSB**") issued its second formal decision in response to noyb's 101 complaints in relation to transfers of personal data from Google Analytics to the United States.[34] The DSB held that the use of Google Analytics on websites operated by Austrian companies, which involved a transfer of personal data to Google LLC in the US, was in breach of Art 44 GDPR as neither the legacy SCCs, nor the supplementary measures implemented, provided an adequate level of protection. In its decision, the DSB did not impose a fine. However, it stated that the relevant website operators must stop using Google Analytics. The DSB specifically considered whether the EU GDPR allows for a risk-based approach to international data transfers, and held that Chapter V GDPR does not recognise a risk-based approach, as it is not provided for in the wording of Art 44 (or, implicitly, anywhere else in Chapter V GDPR).

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

30 DLA Piper has developed a methodology and toolkit to support organisations to carry out transfer impact assessments which are now required by law in most circumstances when exporting personal data from Europe to "third countries". For more information, please visit https://www.dlapiperoutsourcing.com/tools/dla-piper-transfer.html.

31 In August 2020, multiple complaints were filed by noyb against a wide range of data exporters across Europe for their continued transfer of personal data to Facebook and Google in the US in reliance on Article 46 and the SCCs, allegedly in breach of Chapter V GDPR. Details of noyb's 101 complaints are available at www.noyb.eu.

32 The European data protection practices of DLA Piper and Clifford Chance have published a joint paper which argues the case for proportionality and a risk-based approach to international transfers. The paper argues that the European Charter of Fundamental Rights, the Treaty on European Union, the GDPR and relevant CJEU case law do not just permit but *require* a proportionate, risk-based approach to personal data transfers to third countries outside the EEA, which can be implemented in practice and which will help to address the legal uncertainty created by an unlawful strict interpretation of *Schrems II* and Chapter V of the GDPR. The Paper is available here: https://blogs.dlapiper.com/privacymatters/the-gdpr-international-data-transfer-regime-the-case-for-proportionality-and-a-risk-based-approach/.

33 See: Austrian (DSB) decisions available at: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf and https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt%20EN.pdf. French (CNIL) decision available at: https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf. Italian (Garante) decision available at: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782874#english (document: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782890). Danish decision available at: https://www.datatilsynet.dk/english/google-analytics/use-of-google-analytics-for-web-analytics.

34 See: https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt%20EN.pdf.

- In France, in February 2022, the CNIL, in cooperation with other EU data protection supervisory authorities under the GDPR cooperation procedure, analysed the conditions under which data collected through the use of Google Analytics was transferred to the United States and the risks arising for the individuals concerned.[35] The CNIL issued a formal notice to a French website ordering it to comply with the GDPR, holding that the website's processing and transfer of personal data to the U.S. using Google Analytics was in breach of Article 44 GDPR. As with the decision by the Austrian DSB, the CNIL's investigation resulted from noyb's 101 complaints, which included complaints against various websites in France using Google Analytics. The decision of the CNIL is substantively similar to the DSB decision. The CNIL held that transfers of personal data to the United States through Google Analytics undermined the level of personal data protection of data subjects as guaranteed in Article 44 of the GDPR and ordered the website operator to make its data processing compliant with the GDPR within one month from the formal notice. In the CNIL's "Q&A on the formal notices concerning the use of Google Analytics",[36] the CNIL specifically states that controllers cannot adopt a risk-based approach, taking into account the likelihood of data access requests. Similar decisions have followed from the Italian Garante[37] and the Danish Datatilsyne.[38]

These decisions are limited to their facts and are not necessarily representative of the approach taken by all EU data protection supervisory authorities. Decisions to permit transfers which find no infringement of the GDPR are by their nature very unlikely to be published. These decisions all involved the transfer of relatively low-risk data, including IP addresses, other user identifiers, and browser parameters used to provide Google Analytics. The data protection supervisory authorities argued that, since Chapter V GDPR does not specifically refer to proportionality or risk assessment, the principles do not apply to it; and that other references to a risk-based approach and proportionality in the GDPR, such as in Article 24 (in relation to measures to ensure and demonstrate compliance with the GDPR), are not applicable to Chapter V. The data protection supervisory authorities therefore concluded that various transfers made on the basis of the SCCs were unlawful and that a risk-based approach was not permitted when applying Article 46 GDPR. The authors of this survey respectfully disagree with this analysis. There are good arguments that a risk-based approach is not only permitted *but legally required* under Chapter V GDPR and in light of the well-established principle of proportionality enshrined in the Treaty on European Union,[39] the European Charter of Fundamental Rights[40] and leading authorities of the Court of Justice of the European Union.

35 See: https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply.

36 See: https://www.cnil.fr/en/qa-cnils-formal-notices-concerning-use-google-analytics.

37 See: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782874#english (document: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782890). Danish decision see: https://www.datatilsynet.dk/english/google-analytics/use-of-google-analytics-for-web-analytics.

38 See: https://www.datatilsynet.dk/english/google-analytics/use-of-google-analytics-for-web-analytics.

39 Treaty on European Union 2008/C 115/1, see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2008:115:TOC.

40 Charter of Fundamental Rights of the European Union 2012/C 326/02. See: https://ec.europa.eu/info/aid-development-cooperationfundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en.

US ADEQUACY?

On 7 October 2022, President Biden issued an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities ("**the EO**"),[41] aimed at addressing the widespread legal uncertainty that has prevailed with respect to transatlantic data transfers since the *Schrems II* decision. Following last spring's joint US-EU announcement[42] of a "deal in principle" on an enhanced EU-U.S. Privacy Shield Framework ("**Privacy Shield**"), the EO directs US intelligence agencies to take steps to implement US commitments under the renamed EU-U.S. Data Privacy Framework ("**the DPF**").

Following the EO on 13th December, the European Commission published a draft adequacy decision to enhance and replace its 2016 adequacy decision for the Privacy Shield. The Commission has submitted the draft decision to the EDPB for its opinion, and currently expects a committee of EU Member State representatives to approve the draft before July 2023 (the third anniversary of the *Schrems II* ruling). In parallel, the European Parliament has a right of scrutiny and comment on the draft decision (but no ability to change or reject the decision itself). Once these steps have been completed, the Commission can formally adopt the final adequacy decision.

An EU adequacy decision would restore some near-term clarity and predictability around transatlantic data transfers - entities that certify to the DPF are deemed to guarantee a level of protection "essentially equivalent" to that ensured in the EU. U.S. Entities processing personal data under the DPF will no longer need to sign Standard Contractual Clauses ("**SCCs**") or conduct the case-by-case transfer impact assessments ("**TIAs**") imposed for personal data transfers from the EU to the U.S. following the *Schrems II* ruling. For companies eligible for DPF certification, the adequacy determination will significantly ease their compliance burdens.

For companies without DPF certification, SCCs will likely remain the default transfer mechanism. While TIAs will still be required for these transfers as this is mandated in Clause 14 of the SCCs themselves, the recognition in the draft adequacy decision that the U.S. now has in place appropriate legal safeguards relating to government intelligence gathering activities should limit the need to review this element of the legal equivalency test as part of the TIA process.

SCHREMS III?

The long-term durability of any new US adequacy decision remains unclear. While EU Commissioners and U.S. officials are confident the new adequacy decision will address the concerns with US law raised in *Schrems II*, such a decision is all but certain to find its way back to the CJEU for review based on a variety of alleged shortcomings. Max Schrems, has long made clear his expectation that, absent any US *legislative* changes (rather than via an executive order) to address the CJEU's concerns, noyb (or another group) will bring new legal challenges within months of any final adequacy decision. 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 will now issue 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. The European Parliament may also elect to issue its own non-binding resolution on the draft adequacy decision for the DPF at any point before the European Commission formally adopts it.

41 See: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

42 See: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

Commentary

There continues to be a very significant increase in the aggregate value of fines issued across the countries surveyed, jumping from EUR1.09bn (USD1.16bn/GBP0.9bn) for the year starting January 2021 to EUR1.64bn (USD1.74bn/GBP1.43bn) for the year starting 28 January 2022. With five large fines this year against Meta IE,[43] Ireland unsurprisingly takes the top spot in the country league table for the total value of GDPR fines imposed since the application of GDPR on 25 May 2018 to date with aggregate DPC fines exceeding EUR1.3bn (USD1.38bn/GBP1.13bn). Luxembourg remains at the top of the league table for individual fines but has now dropped into second place in the country league table for the total value of fines issued, behind Ireland. As Ireland and Luxembourg are popular locations for technology companies to establish their European operations and as the technology sector remains in the regulatory cross hairs, we anticipate that Luxembourg and Ireland are likely to stay at or near the top of the league table for fines in the coming years.

The notable emerging trend this year is the continuing inflationary influence of the EDPB. Under Articles 60 and 63 GDPR, data protection authorities may refer issues that implicate multiple Member States to the EDPB to adopt a binding decision in accordance with Article 65. In the three binding decisions resulting in administrative fines made by the EDPB since 28 January 2022,[44] the EDPB has increased the originally proposed fine by an average of 630%. It is evident that forum shopping – seeking to establish in Member States which have historically been more hesitant than others to impose large fines – is likely to be less effective going forward in light of the cooperation and consistency mechanism and the willingness of supervisory authorities to use it to object to decisions which they deem to be too lenient.

Enforcement trends

Continuing the trend seen last year, supervisory authorities prioritised enforcement relating to breaches of the core data protection principles in Article 5 GDPR, notably failures to comply with the lawfulness, fairness and transparency principle (Article 5(1)(a)) and the integrity and confidentiality principle (Article 5(1)(f)).

BREACH OF INTEGRITY AND CONFIDENTIALITY PRINCIPLE

This year there were multiple fines issued by data protection supervisory authorities for breach of the integrity and confidentiality principle. For example, the UK ICO issued a fine of GBP4.4m (EUR5m/USD5.3m) against Interserve Group Limited for failing to implement appropriate technical and organisational measures to secure personal data (in contravention of Articles 5(1)(f) and 32 GDPR) for a period of ~20 months. Central to the decision (and another identified recurring point of failure) was that although extensive information security policies and standards were in place, the ICO determined that these policies were not implemented and nor were they subject to appropriate oversight (despite the fact the executive leadership were aware of issues).

While policies and procedures are an essential part of any compliance programme as the "paper shield", without the resources and budgets needed to implement and oversee them effectively, they can become a liability for organisations providing an easy way for data protection supervisory authorities to prove breach.

43 See: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry; https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-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.

44 *Ibid*.

BREACH OF THE PRIVACY BY DESIGN AND DEFAULT PRINCIPLE

In the DPC's recent decision to impose a EUR265m (USD281m/GBP231m) fine[45] against Meta IE (Facebook), the DPC examined the implementation of technical and organisational measures pursuant to Article 25 GDPR and found that Meta IE's measures were insufficient. As a result, in addition to imposing a financial penalty, the DPC also imposed a reprimand and an order requiring Meta IE to bring its processing into compliance by taking a range of specified remedial actions within a particular timeframe. A requirement to remediate controls within a shortened timeline can add significantly to the costs of dealing with the fallout of a regulatory investigation.

FAILURE TO DEMONSTRATE A LAWFUL BASIS TO PROCESS

The DPC's record fine of EUR405m (USD429m/GBP352m) against Meta IE (Instagram) is the first EU-wide decision on children's data protection rights and highlights the special protection merited with regards to the processing of children's personal data. The DPC's Draft Decision[46] was referred to the EDPB under Article 65 of the GDPR (Dispute resolution by the Board) for a binding decision. The DPC had proposed in the Draft Decision to impose nine administrative fines within the total range of EUR202m to EUR405m.[47] The final Decision,[48] which adopts the EDPB's binding decision, contains important lessons and interesting nuances as to how Articles 5(1)(a) and (c), 6(1), 12(1), 25(1) and 35(1) GDPR should be complied with. The EDPB's analysis of Article 6(1) is particularly noteworthy. In particular, the EDPB considered that a legitimate interest pursued by a controller must be determined in a sufficiently clear and precise manner and be real and present, corresponding to current or future activities or benefits. In evaluating the risks of intrusion on the data subject's rights, the EDPB stated that the decisive criterion is the intensity of the intervention for the rights and freedoms of the individual. Given the lack of appropriate measures to address the risks (e.g. the risk of communication between child users and dangerous individuals, the lack of proper information to data subjects regarding publication and its consequences and the impossibility to opt-out from the publication), the legitimate interests pursued were overridden by the interests and fundamental rights and freedoms of child users. However, the EDPB made clear that it is not impossible for a controller to rely on Article 6(1)(f) GDPR where the requirements of the GDPR are met and that a well-designed and workable mechanism for opt-out could play an important role in safeguarding the rights and interests of the data subjects, which may provide a degree of comfort to service providers who are wondering how to legitimise the harvesting of consumer data following the recent DPC decisions against Meta IE.

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

46 See: https://www.dataprotection.ie/en/news-media/latest-news/irish-dpc-submits-article-60-draft-decision-inquiry-instagram.

47 See: https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf. Specifically, on the basis of the DPC's findings in the Draft Decision, the following fine amount ranges were envisaged in respect of the infringements: 1) For the infringement of Art. 12(1) GDPR regarding the public-by-default processing (Finding 1), a fine of between EUR55m and 100m; 2) For the infringement of Art. 12(1) GDPR regarding the contact information processing (Finding 2), a fine of between EUR46m and 75m; 3) For the infringement of Art. 5(1)(a) GDPR regarding the contact information processing (Finding 4), a fine of between EUR9m and 28m; 4) For the infringement of Art. 35(1) GDPR regarding the contact information processing (Finding 5), a fine of between EUR28m and 45m; 5) Infringement of Art. 35(1) GDPR regarding the public-by-default processing (Finding 6), a fine of between EUR28m and 45m; 6) For the infringement of Art. 5(1)(c) and 25(2) GDPR regarding the contact information processing (Finding 7), a fine of between EUR9m and 28m; 7) For the infringement of Art. 25(1) GDPR regarding the contact information processing (Finding 8), a fine of between EUR9m and 28m; 8) For the infringement of Art. 5(1)(c) and 25(2) GDPR regarding the public-by-default processing (Finding 10), a fine of between EUR9m and 28m; 9) For the infringement of Art. 25(1) GDPR regarding the public-by-default processing (Finding 11), a fine of between EUR9m and 28m.

48 See: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22022-dispute-arisen_en.

Looking back at our predictions for 2022

In last year's report we predicted that data transfers would continue to be an enforcement priority; that there would be more complaints, investigations and enforcement activity in relation to cookies and similar tracking technologies, and more enforcement in relation to ad-tech. All of these predictions have come to pass though none more emphatically than enforcement in relation to behavioural advertising. There has been a spate of Irish DPC fines. These have the potential to be every bit as profound for the grand bargain between online service providers and consumers, which has funded most of the free to use internet we know today, as *Schrems II* has been for international data transfers.

"There has been a spate of Irish Data Protection Commission fines arising from behavioural advertising practices. These have the potential to be every bit as profound for the grand bargain struck between online service providers and consumers which has funded most of the free to use internet we know today, as Schrems II has been for international data transfers."

PREDICTIONS FOR THE YEAR AHEAD

Our predictions for the year ahead include:

- The battle lines are drawn between online service providers relying on behavioural advertising to fund consumer services and data protection supervisory authorities. We anticipate more enforcement following on from the Irish DPC fines and more appeals. There are many fundamental questions of law relating to behavioural advertising which remain far from settled. While the EDPB concluded on the facts relating to the Facebook decision that Facebook could not rely on contractual necessity[49] as a lawful basis to harvest and profile user personal data in order to be able to serve targeted adverts, it is notable that data protection supervisory authorities were split on this question and it remains to be seen whether contractual necessity could be successfully relied upon where online service providers are clearer in privacy notices and consumer terms and conditions about the nature of the service they are offering.[50] A wider question is whether it is really in the best interests of consumers to undermine the financial model at the heart of the free consumer internet.

49 Article 6(1)(b) GDPR.

50 See: https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland.

- A bumpy ride for the new EU – US adequacy decision. Max Schrems has made no secret of his scepticism that the recently passed US Executive Order fails to address the substantive concerns raised by Europe's highest court in *Schrems II*. It seems almost inevitable that a new EU – US adequacy decision will end up before Europe's highest court before long, though it may survive 2023. Given the uncertainty, organisations should consider alternative options to legitimise personal data transfers as a fallback in case any new adequacy decision fails, such as SCCs coupled with transfer impact assessments[51] or one of the derogations listed in Article 49 GDPR. Transfers will continue to be a legal and compliance minefield for as long as conflicts of laws remain between one country's privacy rights and another's interception powers. Given this uncertainty, the authors of this survey sincerely hope that the proportionality principle will be resurrected after it was prematurely (and in our view illegally) dismissed in some of the early enforcement decisions relating to Google Analytics. It is not in the interests of consumers nor consistent with the freedom to carry on a business enshrined in the European Charter of Fundamental Rights[52] to apply the same absolutist interpretation to all transfers, irrespective whether there is actually any risk of harm arising for the data subject.
- Data protection supervisory authorities will continue to grapple with artificial intelligence. With the EU AI Act expected to be finalised in 2023,[53] we expect more guidance from data protection supervisory authorities on the interplay between AI and data protection law and as part of that the interplay between AI and data ethics. We also predict increased investigations and enforcement into the more invasive and personal data rich AI systems and solutions.

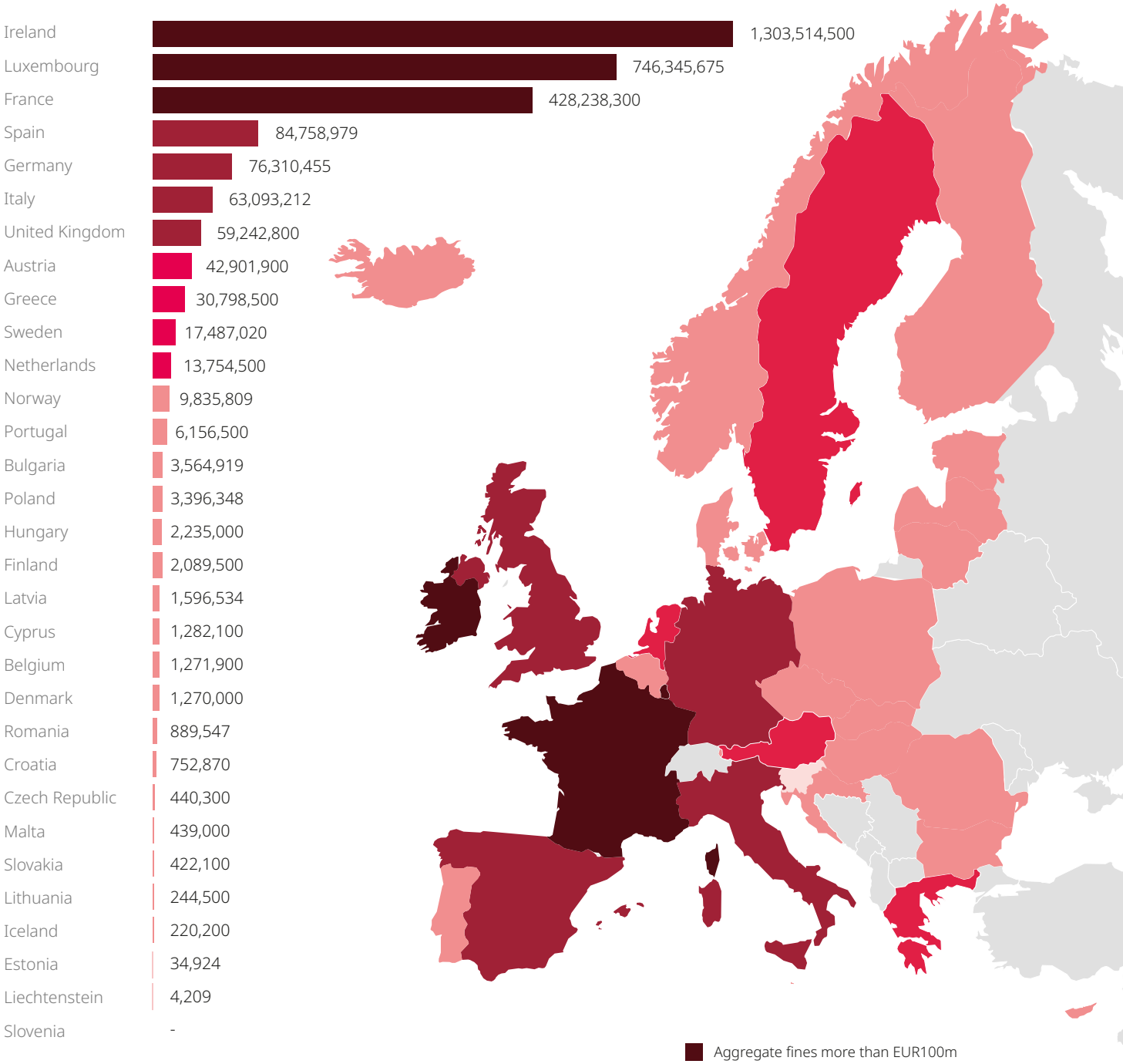
51 Article 46 GPDR. For information about the DLA Piper Transfer tool please see: https://www.dlapiperoutsourcing.com/tools/dla-piper-transfer.html.

52 Article 16 European Charter of Fundamental Rights.

53 See: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf. In December 2022 the European Council adopted its common position (general approach) on the AI Act. The next stage is for the European Council to enter negotiations with the European Parliament ('trilogues'), which is expected in April 2023.

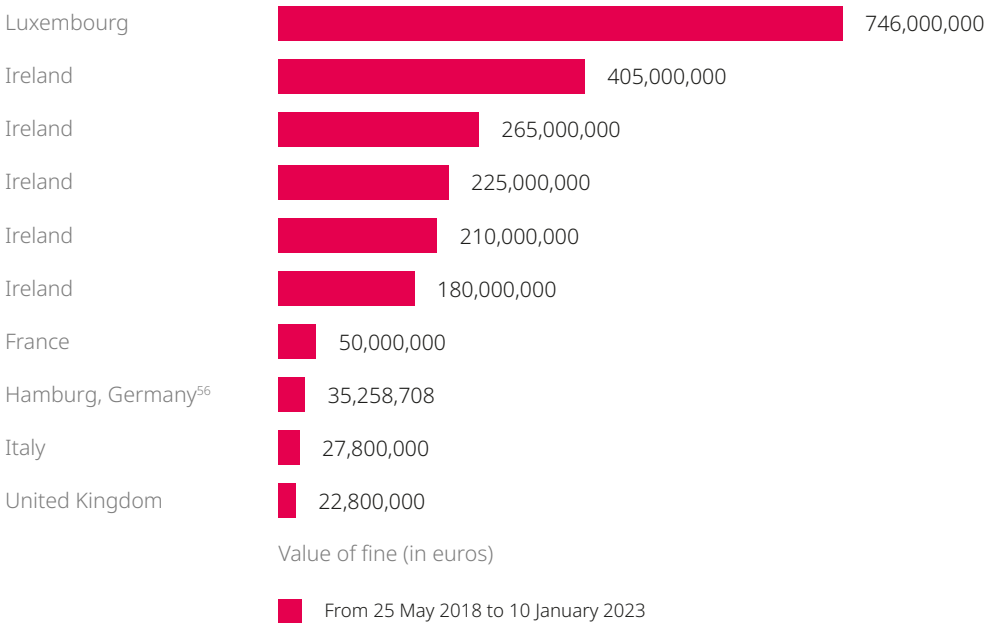
Report

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.

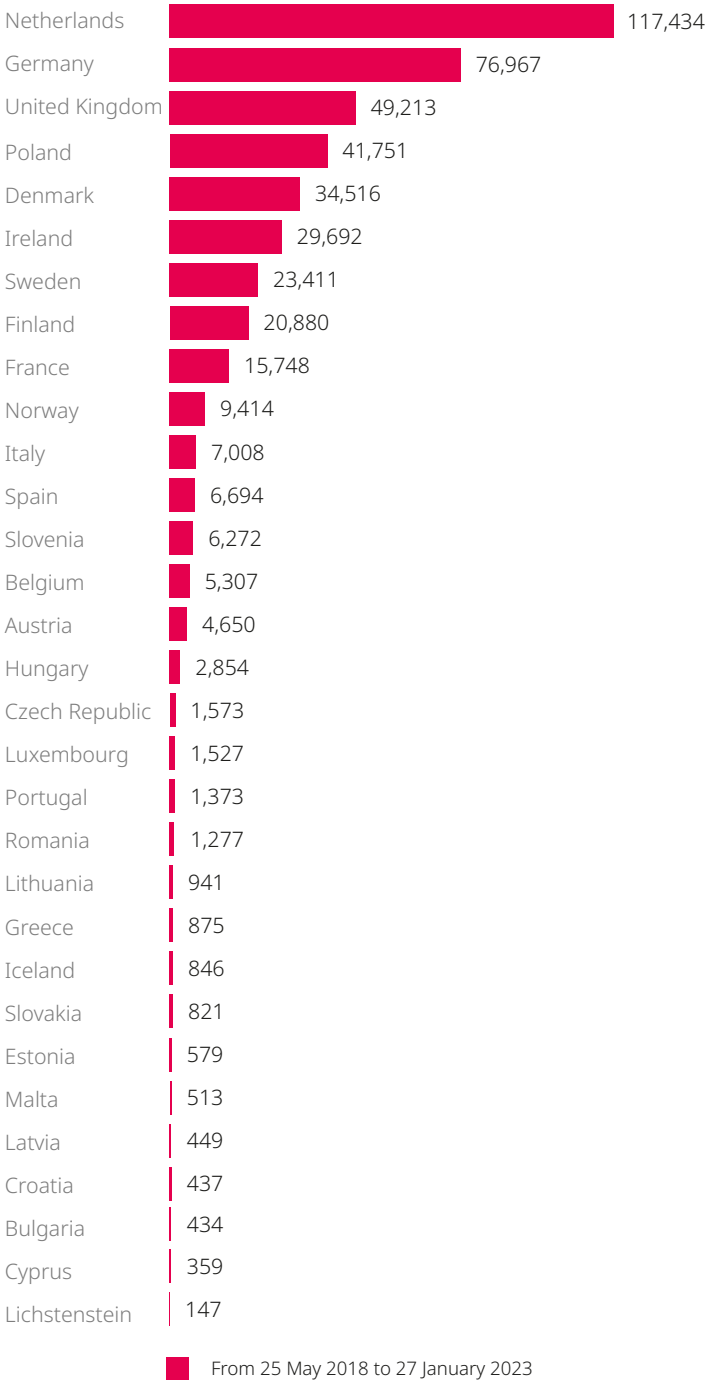
Top ten largest fines imposed to date under GDPR[55]



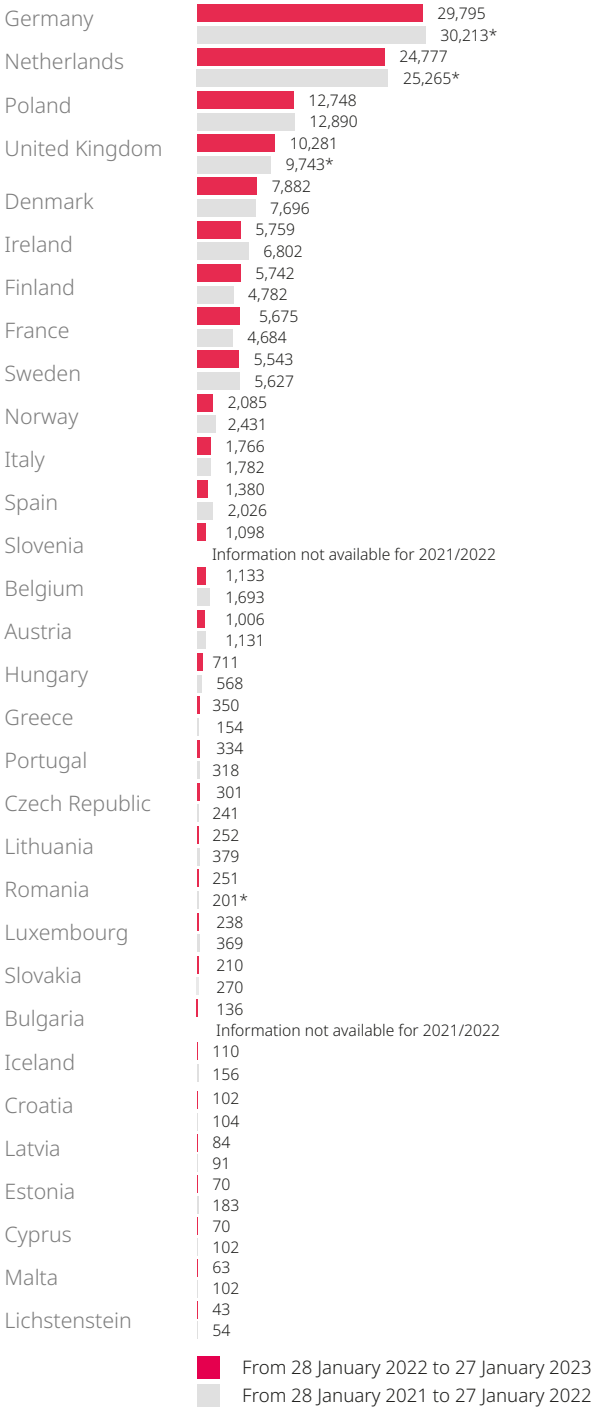
55 This report only includes fines imposed under the GDPR (i.e. it does not include fines imposed under other regimes such as e-privacy legislation).

56 Germany has 16 different state data protection supervisory authorities, plus a federal supervisory authority.

Total number of personal data breach notifications between 25 May 2018 and 27 January 2023 inclusive*

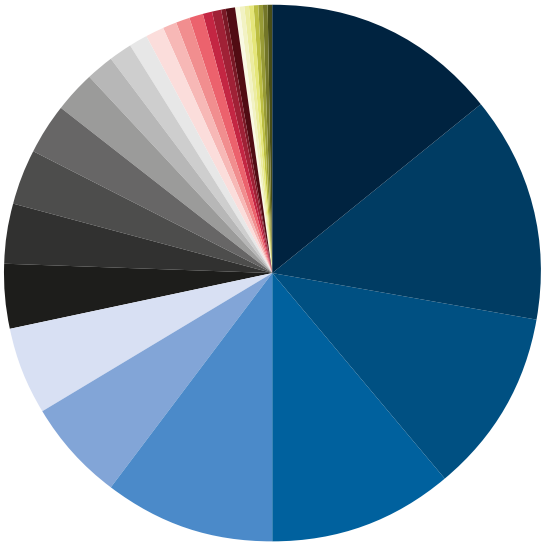


Total number of personal data breach notifications between 28 January 2022 and 27 January 2023 (inclusive last 12 month period)*



*Not all the countries covered by this report are inlcuded 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 (such as for the UK and Germany) 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. 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 2022 and 27 January 2023 (last 12 month period)	Change compared to last year's ranking*
Netherlands	142.39	No change
Denmark	133.13	+1
Lichstenstein	109.18	-1
Ireland	109.17	+1
Finland	102.51	+1
Slovenia	58.92	+1
Sweden	52.87	+2
Norway	37.53	+2
Luxembourg	36.64	-1
Poland	33.47	+2
Iceland	30.63	No change
Germany	24.72	-6
United Kingdom	15.16	+3
Malta	13.62	-1
Austria	11.29	+3
Belgium	9.57	-1
Lithuania	9.39	No change
France	8.3	+3
Hungary	7.33	-1
Estonia	5.8	-6
Cyprus	5.42	-1
Latvia	4.53	+1
Slovakia	3.87	-1
Portugal	3.45	Information not previously publically available
Greece	3.32	+3
Spain	2.93	-2
Italy	2.89	-2
Czech Republic	2.81	-1
Croatia	2.44	-3
Bulgaria	1.9	Information not previously publically available
Romania	1.35	Information not previously publically available



* 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 2022 estimates).
* Full breach notification statistics were not, at the time of publication, publicly available for 2022 in a number of jurisdictions including Germany, the Netherlands and Belgium (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 2021, this may have impacted upon last year's rankings.

Additional resources

The DLA Piper global cybersecurity and data protection team of more than 180 lawyers has developed the following products and tools to help organisations manage their data protection and cybersecurity compliance. For more information, visit dlapiper.com or get in touch with your usual DLA Piper contact.

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 100 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 200 organisations to assess exports of personal data from the UK and EEA to third countries and we now have over 70 comparative assessments of third country laws and practices available. We offer an update service to users of Transfer, which includes regular updates to our tool and third country comparative assessments to keep up-to-date with changes in law and practice.

DLA Piper Privacy Matters Blog

We have a dedicated data protection blog, *Privacy Matters*, where members of our global team post regular updates on topical data protection, privacy and security issues and their practical implications for businesses. Subscribe to receive alerts when a new post is published.

DLA Piper Data Privacy Scorebox

Our Data Privacy Scorebox helps to assess an organisation's level of data protection maturity. It requires completing a survey covering areas such as storage of data, use of data, and customers' rights. A report summarising the organisation's alignment with 12 key areas of global data protection is then produced. The report also includes a practical action point checklist and peer benchmarking data.

DLA Piper Notify: Data Breach Assessment Tool

We have developed an assessment tool, known as Notify, that allows organisations to assess the severity of a personal data breach, using a methodology based on objective criteria from official sources to determine whether or not a breach should be notified to supervisory authorities and/or affected individuals.

The tool automatically creates a report that can be used for accountability purposes as required by GDPR.