GDPR Fines and Data Breach Survey: January 2022

This is the fourth annual DLA Piper fines and data breach survey since the application of the EU General Data Protection Regulation ("GDPR") on 25 May 2018.

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.

It has been another busy period for enforcement with new record-breaking fines taking the top two spots on the GDPR fines league table and several notable court and supervisory authority decisions. Organisations and privacy professionals have also been kept busy this year dealing with the fallout of the decision by the Court of Justice of the European Union ("CJEU") in the case known as Schrems II.[1] The judgment has profound implications for transfers of personal data from Europe to "third countries". Recent case-law in France potentially expands this challenge to cloud services hosted entirely within Europe where they are provided by vendors subject to third country interception laws. Data localisation may not be sufficient to address Schrems II.

With thanks to the many different contributors and supervisory authorities who make this report possible,[2] our fourth annual survey takes a look at key GDPR metrics across the European Economic Area ("EEA") and the UK[3] since GDPR first applied and for the year commencing 28 January 2021. The EEA includes all 27 Member States of the EU plus Norway, Iceland and Liechtenstein.

There has been a sevenfold increase in GDPR fines this year with just under EUR1.1bn (USD1.2bn/GBP0.9bn)[4] fines imposed since 28 January 2021 compared to EUR158.5m (USD179m/GBP132m) during the same period last year.[5]

Fines may be grabbing the headlines but the Schrems II judgment and its profound implications for data transfers continues to be a major challenge for organisations caught by GDPR.

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

2 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, Schellenberg Wittmer Ltd and Sorainen for their contributions in relation to Liechtenstein, Croatia, Bulgaria, Greece, Iceland, Malta, Cyprus, Switzerland, Estonia, Latvia and Lithuania respectively.

3 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 2022. It remains to be seen the extent to which these changes will deviate from the EU GDPR.

4 In this report we have used the following exchange rates: EUR 1 = USD 1.13/GBP 0.83.

5 This survey only covers GDPR fines so does not include fines imposed under other regimes, such as the two large fines recently imposed by the CNIL on Meta and Google for EUR60m and EUR150m respectively for infringements of the e-Privacy Directive as implemented under French law.

SUMMARY AND KEY FINDINGS

Record-breaking New Fines

This year has seen two record breaking GDPR fines.[6] The first was imposed by the Luxembourg data protection supervisory authority against a US based online retailer and e-commerce platform for EUR746m (USD843m/ GBP619m). The second was imposed by the Irish Data Protection Commission on WhatsApp Ireland Limited for EUR225m (USD254/GBP187m). Both fines are subject to ongoing appeals.[7]

Sevenfold Increase in Value of Aggregate Fines Imposed

This year supervisory authorities across Europe have issued[8] a total of EUR1.087bn (USD1.23bn/GBP0.9bn) in fines since 28 January 2021, which is a sevenfold increase on the total of EUR158.5m (USD179m/ GBP132m) issued in the year from 28 January 2020. Much of this increase is due to the two record-breaking fines referenced above. Fines may be grabbing the headlines but the Schrems II judgment and its profound implications for data transfers continues to be a major challenge for organisations caught by GDPR.

Country Aggregate Fines League Table

It's all change at the top of this year's country league table for the aggregate fines imposed to date with Luxembourg and Ireland replacing Italy and Germany in the top two spots and Italy moving down to third place with EUR746m (USD843m/ GBP619m), EUR226m (USD255m/ GBP188m) and EUR79m (USD89m/ GBP66m) respectively.

Significant Increase of Breach Notifications

The trend of increasing numbers of data breach notifications has also continued over the last year. For the year commencing 28 January 2021, there have been more than 130,000 personal data breaches notified to regulators and on average 356 breach notifications per day, an 8% increase on last year's daily average of 331 notifications.[9]

Successful Appeals

This year has also seen some successful appeals against decisions and penalties imposed by data protection supervisory authorities. Notably, the German data protection supervisory authorities are continuing to find difficulties in making fines stick. The headline EUR14.5m (USD16.4m/ GBP12m) fine imposed by the Berlin data protection supervisory authority against Deutsche Wohnen SE for alleged infringements of the storage limitation principle was held to be invalid by the Regional Court of Berlin on the basis that the Berlin DPA failed to specify acts of the management of Deutsche Wohnen SE which were in breach of GDPR and therefore did not satisfy the requirements of the German Act on Regulatory Offences.[10] The public prosecutor in consultation with the Berlin DPA has now appealed the Regional Court's decision. This follows a decision by the Bonn Regional Court in November 2020 reducing a EUR9.6m (USD10.8m/GBP8m) fine against 1&1 Telecom on the basis the original fine was "unreasonably high". As noted in last year's survey following the 90% and 80% reductions of the fines originally proposed by the UK ICO for two data breaches, given there is so much legal uncertainty and so many open legal questions concerning GDPR, it often pays to appeal and to mount robust challenges to proposed regulatory sanctions.

6 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.

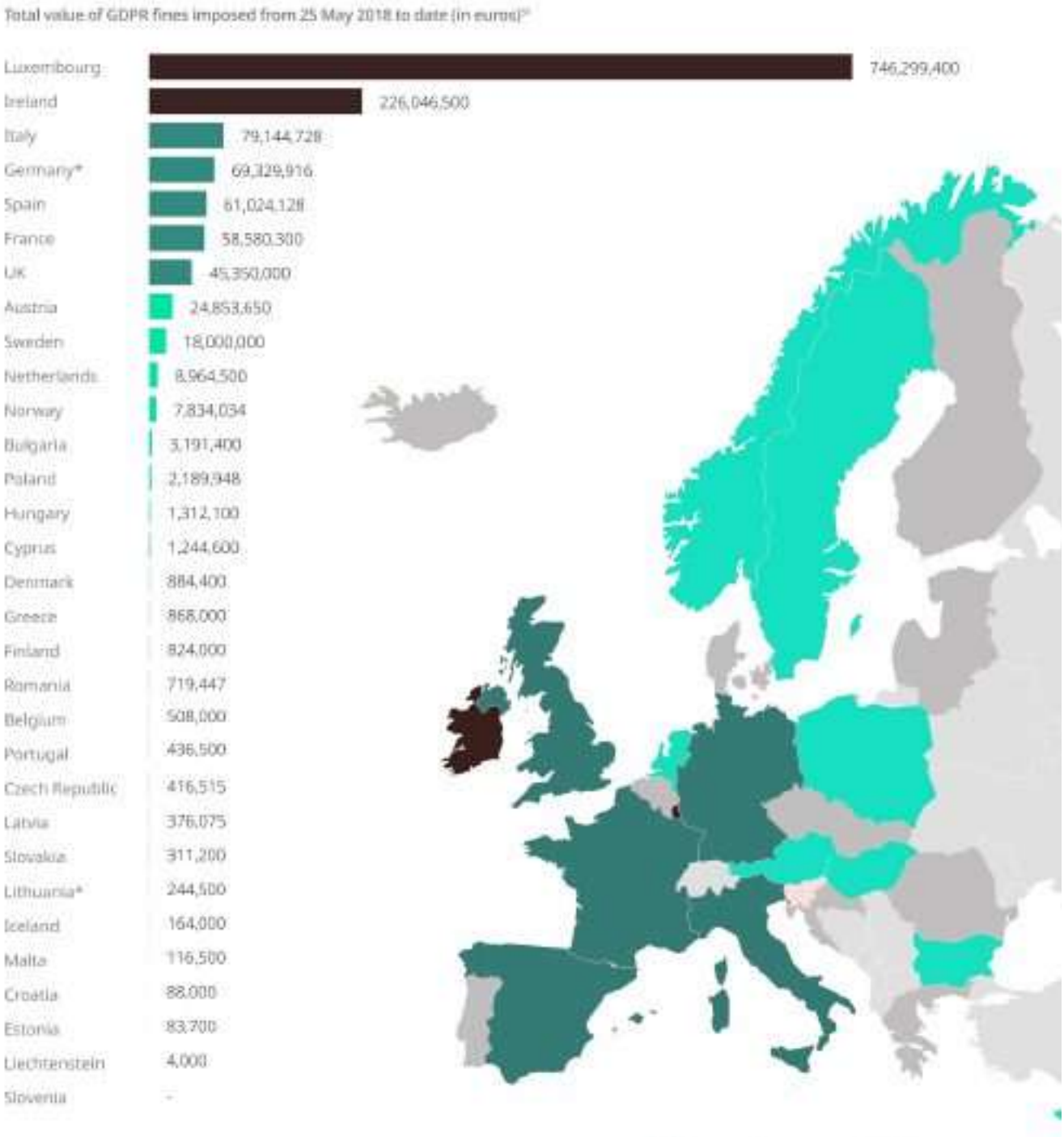
7 WhatsApp has applied to the Court of Justice of the European Union to annul the decision of the European Data Protection Board. A summary of the grounds of appeal is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021TN0709&from=EN.

8 Not all supervisory authorities publish details of fines. Some treat them as confidential. Our report 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.

9 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, including Germany, which has previously had high numbers of data breach notifications. 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.

10 There is ongoing debate in Germany whether the German Act on Regulatory Offences, which requires proof of specific acts of infringement by the management of legal persons, is consistent with GDPR, which includes no such requirement when imposing fines.

Report



* Not all information in relation to fines by the different German DPAs is made publically available, therefore the real figure is likely to be higher than reported.

* In Lithuania, data in relation to minor fines imposed is not available and therefore the figure provided does not include the value of minor fines.

[1] This report does not include fines that have been successfully appealed.

HIGHEST INDIVIDUAL FINE LEAGUE TABLE

#1

Luxembourg – €746m

Luxembourg's data protection supervisory authority, the CNPD, takes pole position this year with a fine of EUR746m (USD843m/ GBP619m) against a US online retailer and e-commerce platform. The fine is not publicly available and is subject to an ongoing appeal.

#2

Ireland– €225m

On 2 September 2021 the Irish Data Protection Commission ("DPC") issued a fine of EUR225m (USD254m/GBP187m) against WhatsApp Ireland Limited for various findings of failings to comply with the GDPR transparency requirements as well as a reprimand and order to bring its processing into compliance. WhatsApp has appealed to the CJEU to annul the decision (Articles 5(1)(a), 12, 13 and 14 GDPR).

#3

France – €50m

The Luxembourg and Irish fines have moved last year's top fine issued by France's data protection supervisory authority, the CNIL, into third place. The CNIL fined Google EUR50m (USD56.5m/GBP41.5m) for various findings of failings to comply with transparency requirements and for failing to have an adequate legal basis for processing in relation to personalised advertising (Articles 5, 6, 13).

SCHREMS II FALLOUT

The decision of Europe's highest court in Schrems II in July 2020 was seismic. The CJEU invalidated the Privacy Shield regime and left standard contractual clauses on life support – which are by far the most common mechanisms to legitimise transfers of personal data from Europe. It was also expressly stated that a controller established in the EU and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned.

On 18 June 2021 the European Data Protection Board finalised its recommendations on how organisations should comply with the judgment. These are not legally binding but will be followed by supervisory authorities to inform enforcement decisions and will carry weight in the courts. Among other things, the recommendations require comprehensive mapping of data transfers and transfer impact assessments where individual transfers rely on standard contractual clauses or binding corporate rules.

In June 2021 the European Commission helped to reduce the compliance gap to some extent by issuing updated standard contractual clauses which take into account the EDPB recommendations so far as they relate to contractual supplementary measures. However, these new clauses still require organisations to complete transfer impact assessments and may not be sufficient to achieve equivalent protection without additional organisational and technical measures.

Meeting the requirements of Schrems II and the EDPB recommendations is a very significant undertaking requiring a complicated assessment of the laws and practices of typically multiple third countries to which personal data are transferred or can be accessed from. It is a challenge even for the most sophisticated and well-resourced organisations and is beyond the means of many small and medium-sized enterprises.