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

DLA Piper GDPR data breach survey: January 2020

DLA PIPER

DLA Piper GDPR data breach survey: January 2020

The EU General Data Protection Regulation (GDPR) came into force across the European Union on 25 May 2018. In February 2019 DLA Piper published the first DLA Piper Data Breach Survey covering the first 8 months of the GDPR regime to 27 January 2019. With thanks to the many different contributors and supervisory authorities who make this report possible, our 2020 report takes a look at key GDPR metrics across the European Economic Area ("EEA") 12 months on. The EEA includes all 28 Member States of the EU plus Norway, Iceland and Liechtenstein.

Organisations face stiff penalties for failing to notify personal data breaches within the stipulated time periods including fines of up to €10 million, or up to 2% of the total worldwide turnover of the preceding financial year, whichever is higher.

Under the GDPR personal data breaches that are likely to result in "a risk" to the rights and freedoms of natural persons must be notified by the "controller" organisation to the appropriate data protection supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where a personal data breach is likely to result in a "high risk" to the rights and freedoms of natural persons, these individuals must also be notified without undue delay.

Organisations face stiff penalties for failing to notify personal data breaches within the stipulated time periods including fines of up to €10 million, or up to 2% of the total worldwide turnover of the preceding financial year, whichever is higher.

Many organisations and indeed many supervisory authorities are struggling with how to determine when a breach is or is not notifiable given the vagaries of the legal trigger for notification – where there is "a risk" to the rights and freedoms of natural persons. Neither term is defined in the GDPR. Some guidance is available including, at an EU level, the Guidelines on Personal Data Breach Notification which were originally published by the Article 29 Working Party and subsequently adopted by the European Data Protection Board. However, the guidance is high level and open to wide interpretation. Further guidance would be welcomed both by organisations reporting breaches and supervisory authorities assessing breaches in order to drive consistency and best practice for risk assessment. A consistent approach would also help supervisory authorities across the EU to triage and identify the most serious personal data breaches more quickly.

This year's report takes a closer look at the number of breaches notified to data protection supervisory authorities, the fines that have been issued and evolving trends.

Summary and key findings

From 25 May 2018 to 27 January 2020 there have been a total of 160,921 personal data breaches notified by organisations to data protection supervisory authorities within the EEA.

For the period from 25 May 2018 to 27 January 2019 there were on average 247 breach notifications per day. For the period from 28 January 2019 to 27 January 2020 there were on average 278 breach notifications per day (a 12.6% increase), so the current trend for breach notifications is upwards.

Details of breaches notified are not made public as a default but it is likely that a wide spectrum of data breaches have been notified from fairly minor errant emails mistakenly sent to the wrong address to the most serious criminal cyber attacks affecting millions of individual records.

The Netherlands, Germany and the UK had the most data breaches notified for the 20 months from 25 May 2018 to 27 January 2020, with 40,647, 37,636 and 22,181 respectively. The Netherlands, Germany and the UK also topped the table for the total number of breach notifications in last year's report.

The countries with the fewest breaches notified for the full 20 month period were Latvia, Cyprus and Liechtenstein with around 173, 94 and 30 respectively. Last year, Cyprus, Iceland and Liechtenstein came bottom of the table.

When the results are weighted to take into account country population, The Netherlands retains its top ranking with the most breaches notified per 100,000 capita. Ireland and Denmark also retain their second and third rankings in the breaches per 100,000 capita table.

The UK, Germany and France rank 13th, 11th and 23rd respectively for the full 20 month period while Italy, Romania and Greece have reported the fewest breaches per capita. Both the UK and France have moved down the rankings compared to last year with a drop of 3 and 2 places respectively. Germany's 11th place ranking remains unchanged compared to last year.

Some notable GDPR fines have been imposed over the last year for a wide range of GDPR infringements, not just relating to data breaches. The UK's Information Commissioner's Office made global headlines when it announced notices of intent to fine companies from the airline and hospitality industries £183 million (about €213 million / $238 million) and £99 million (about €115 million / $129 million) respectively for alleged poor security arrangements and failures to carry out appropriate due diligence though at the time of writing neither of these fines have been finalised. That said, the UK ICO has so far only issued one relatively small fine under GDPR for £275,000 in December 2019 despite having received 22,181 personal data breach notifications to date.

Although data on the number and amount of GDPR fines imposed is not universally available across the jurisdictions surveyed, the UK experience is not atypical. With some notable headline grabbing exceptions, relatively few fines have been imposed under the new GDPR regime. Not all GDPR fines are made public. The total (reported) fines for the full 20 month period across all countries surveyed was just over €114 million (about US$126 million / £97 million) which is quite low given that supervisory authorities enjoy the power to fine up to 4% of total worldwide annual turnover of the preceding financial year. France, Germany and Austria top the table for the total value of GDPR fines imposed to date with €51 million, €24.5 million and €18 million respectively.

It would be unwise to assume that low and infrequent fines will be the norm going forward. Supervisory authorities across Europe have been staffing up their enforcement teams and getting to grips with the new regime. It takes time to build a robust case to justify higher fines. We expect to see more multi million Euro fines in the coming year.

Fines certainly aren't the only potential exposure for organisations which fall short of GDPR's exacting requirements. Supervisory authorities enjoy a wide range of powers to impose other sanctions including in some countries the ability to publicly name and shame the wrongdoer. There is also an increased risk of "follow-on" compensation claims, including group litigation which follow a regulatory finding of liability. Litigation funders have billions of Euros available to fund claims and – where local civil procedure rules permit – are becoming increasingly active pursuing group litigation claims for large groups of affected individuals on the basis of alleged breaches of GDPR and data protection laws. Recent UK group litigation claims based on data protection law infringements would be very familiar to US class action lawyers.

Commentary

A theme of this year's report is that there has been little change at the top of the table. The Netherlands, Germany and the UK retain the top three rankings for the total number of data breach notifications made both over the full 20 month period from GDPR coming into force on 25 May 2018 and for the most recent full year from 28 January 2019 to 27 January 2020. Similarly, the top of the weighted breach notifications per 100,000 capita table remains unchanged with The Netherlands, Ireland and Denmark retaining their top spots. Notably Italy with a population of more than 62 million people only recorded 1886 breach notifications for the full 20 month period from 25 May 2018 retaining its third from bottom ranking for breach notifications per 100,000 capita. The Italian example illustrates that although GDPR as an EU Regulation applies across the entire EU (plus Norway, Iceland and Liechtenstein) its interpretation and application by regulators varies widely making compliance a particular challenge for multi-national organisations.

We have seen the first significant fines under GDPR. The total value of GDPR fines imposed for the full 20 month period across Europe was just over €114 million with France, Germany and Austria topping the table for the value of fines imposed (notably not counting the UK notices of intent to fine). It is still early days and there remains a great deal of uncertainty as to how fines should be properly calculated and imposed under GDPR. The German data protection authorities caused quite a stir in October 2019 when they published guidelines for calculating GDPR fines. The proposed methodology, if followed, would drive much higher fines. Similarly the two notices of intent to fine published by the UK ICO have caused alarm with little apparent correlation between the proposed fine and actual harm caused to individuals. The key takeaway from the early guidance and regulatory skirmishes is that how GDPR fines should be calculated remains an open legal question. It will take time – likely several years if not a decade – before a standard methodology starts to emerge from the jurisprudence of Member State courts, from the European Court of Justice and from the European Data Protection Board. In the meantime, particularly given the size of some of the early fines, we anticipate that appealing fines will become much more common.

GDPR enforcement isn't limited to breach of Article 32 (security of processing). The early GDPR fines demonstrate that supervisory authorities are also targeting failure to comply with the core principles relating to processing of personal data set out in Article 5 GDPR, notably failures to comply with the lawfulness, fairness and transparency principle; failure to comply with the data minimisation principle and failure to comply with the storage limitation principle. Several supervisory authorities have imposed fines on controllers for failing to comply with their obligations relating to the rights enjoyed by data subjects, notably in relation to the right to access personal data.

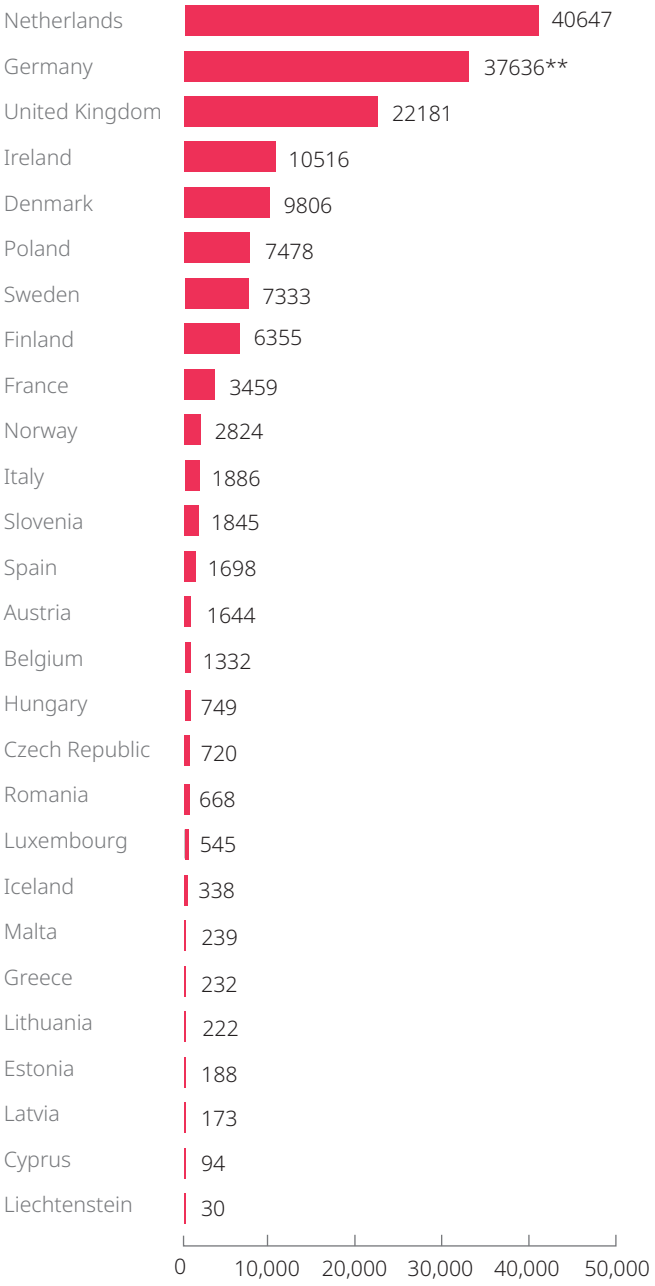
What constitutes appropriate security measures meeting the standard required by Article 32 GDPR is likely to be a key battle ground between the regulators and the regulated in the years ahead. In the same way that encryption became part of the legal standard of care under the previous regime, we anticipate that we will see other security controls emerge as hard requirements under Article 32 GDPR such as multi factor authentication when processing higher risk personal data. As was the case under the previous regime, we also anticipate that the Payment Card Industry Data Security Standard (PCI DSS) will be deemed to form part of the legal standard of care required by Article 32 GDPR when organisations process payment card information.

The approach to publication of details of GDPR enforcement and fines varies significantly among the countries surveyed. In some, the default practice of supervisory authorities is not to publish the name of organisations which have received fines. The authors of this report nevertheless hope that in time supervisory authorities will volunteer more generic information about the nature of fines imposed and the sectors the organisations fined are in, to improve transparency.

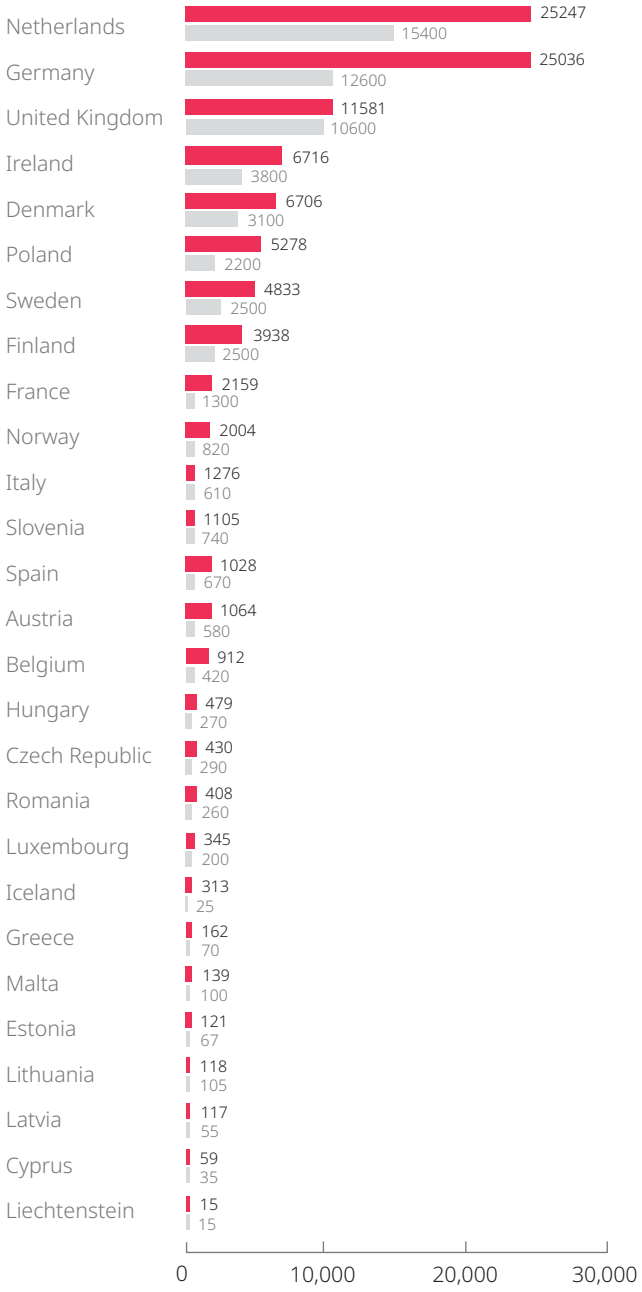
This publication has been prepared by DLA Piper. We are grateful to Batliner Wanger Batliner Attorneys at Law Ltd., Glinska & Mišković, Kamburov & Partners, Kyriakides Georgopoulos, LOGOS, Mamo TCV Advocates, Pamboridis LLC, and Sorainen for their contributions in relation to Liechtenstein, Croatia, Bulgaria, Greece, Iceland, Malta, Cyprus, Estonia, Latvia and Lithuania respectively.

Report

Total number of personal data breaches notified per jurisdiction for the period from 25 May 2018 to 27 January 2020 inclusive*



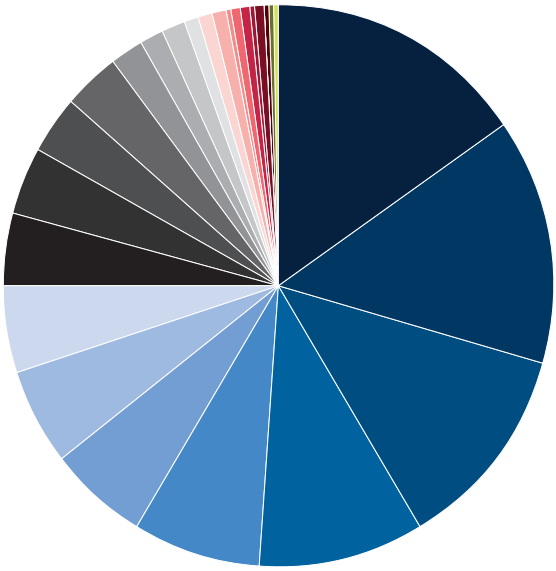
Number of data breaches notified per jurisdiction between 28 January 2019 and 27 January 2020 inclusive



*Not all of the countries covered by this report make breach notification statistics publicly available and many only provided data for 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 pre-dating GDPR.

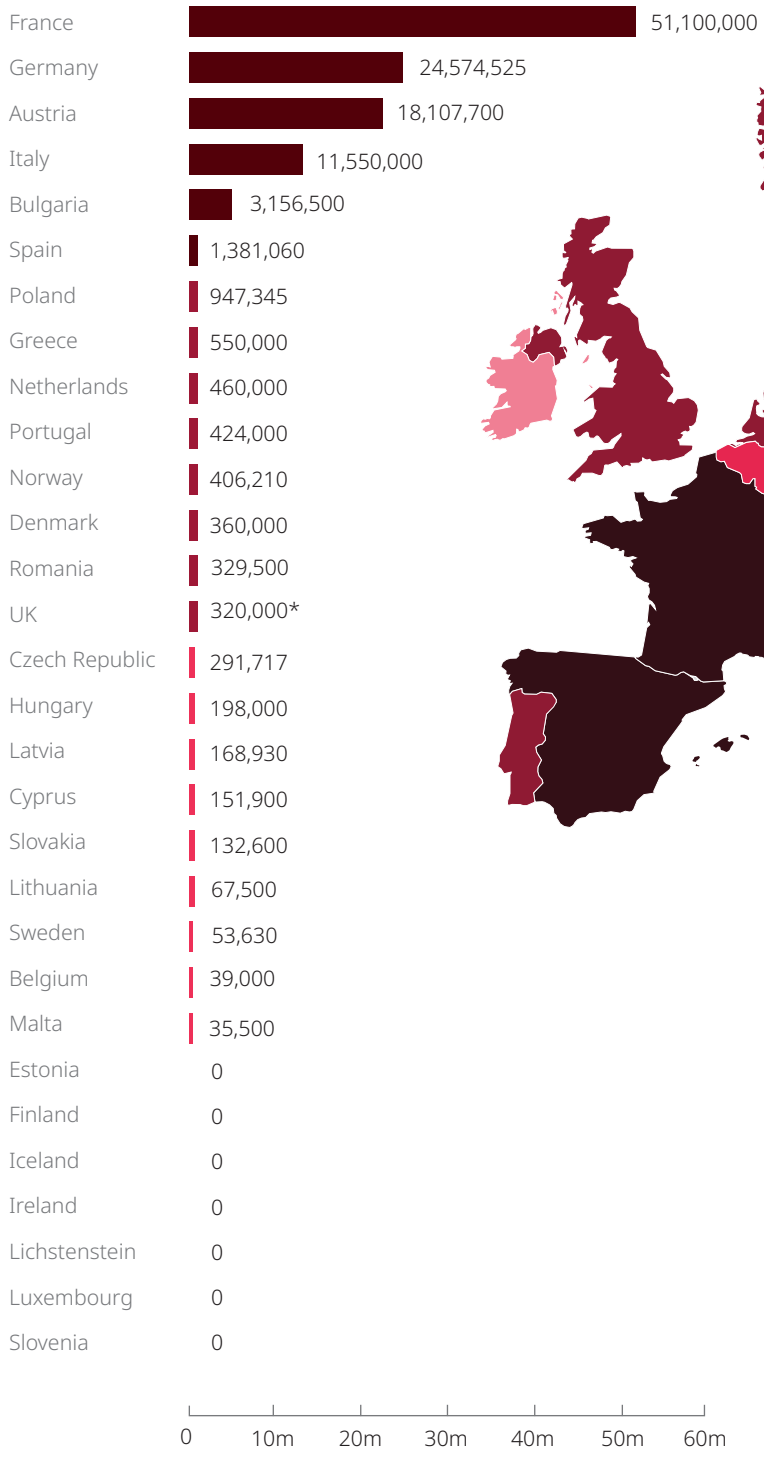
**Germany has 16 different State data protection supervisory authorities plus a federal supervisory authority. The supervisory authorities for Baden-Wuertemberg, Mecklenburg Western Pomerania, Saxony and Saxony-Anhalt either provided incomplete data or no data so we have extrapolated data for these States based on the data provided by other State supervisory authorities.

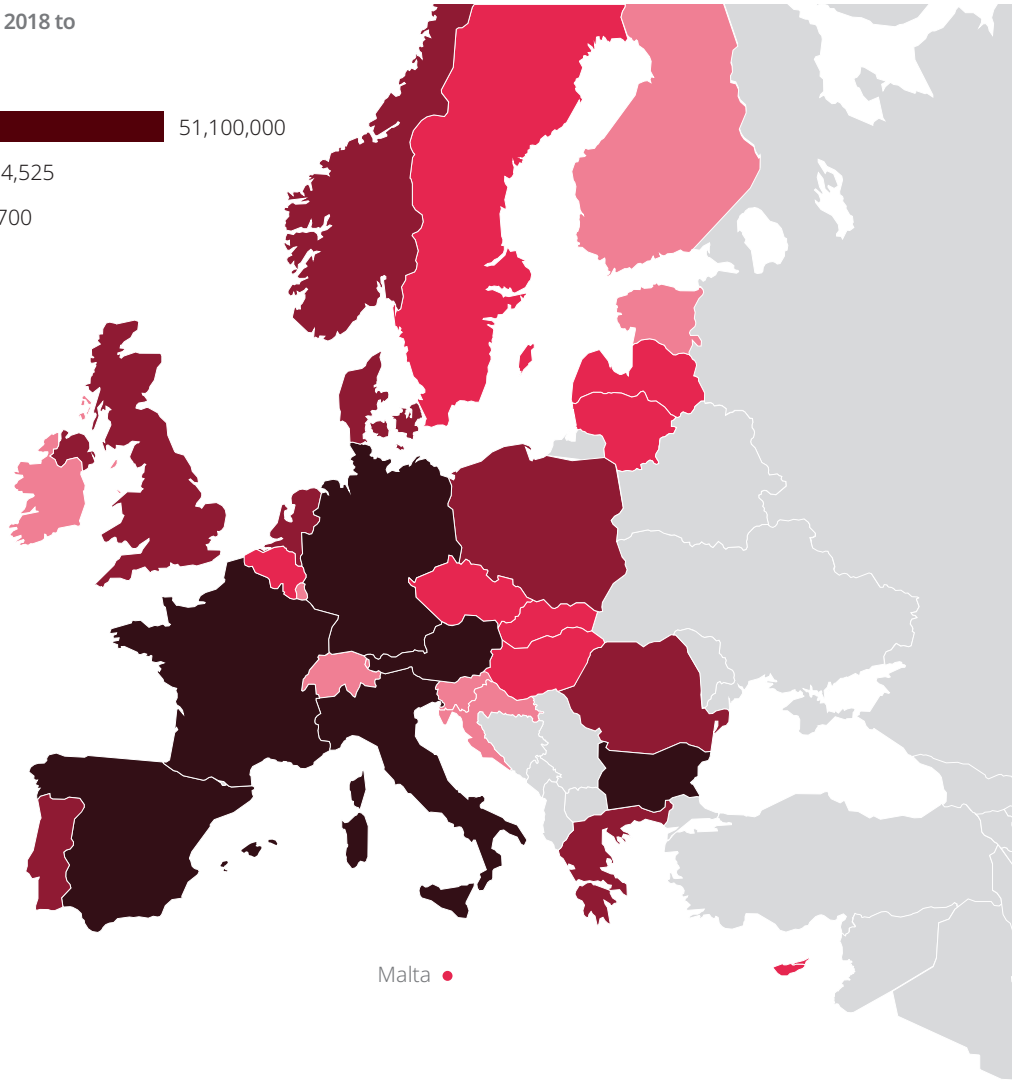
Per capita country ranking of breach notifications*	Number of data breaches per 100,000 people for the period 28 January 2019 to 27 January 2020 inclusive	Change compared to last year's ranking
Netherlands	147.2	0
Ireland	132.52	0
Denmark	115.43	0
Iceland	91.15	+9
Finland	71.11	-1
Luxembourg	56.97	+1
Slovenia	52.55	-1
Sweden	48.14	0
Liechtenstein	39.18	-4
Norway	37.31	+2
Germany	31.12	0
Malta	31	-3
United Kingdom	17.79	-3
Poland	13.74	+1
Austria	12.1	-1
Estonia	9.74	N/A
Belgium	7.88	-1
Latvia	6.13	0
Hungary	4.87	0
Cyprus	4.8	-3
Lithuania	4.18	N/A
Czech Republic	4.03	-2
France	3.2	-2
Spain	2.08	-1
Italy	2.05	0
Romania	1.9	-2
Greece	1.5	-1



*Per capita values were calculated by dividing the number of data breaches reported 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 2018 estimates)

Total value of GDPR fines imposed from 25 May 2018 to 17 January 2020 in Euros





- Aggregate fines more than 1 million Euros
- Aggregate fines between 300,000 and 1 million Euros
- Aggregate fines up to 300,000 Euros
- No fines reported

*The UK figures do not include the two public notices of intent to fine totalling £282 million (about €329 million / $366 million) as they had not been finalised and imposed at the time of writing this report.