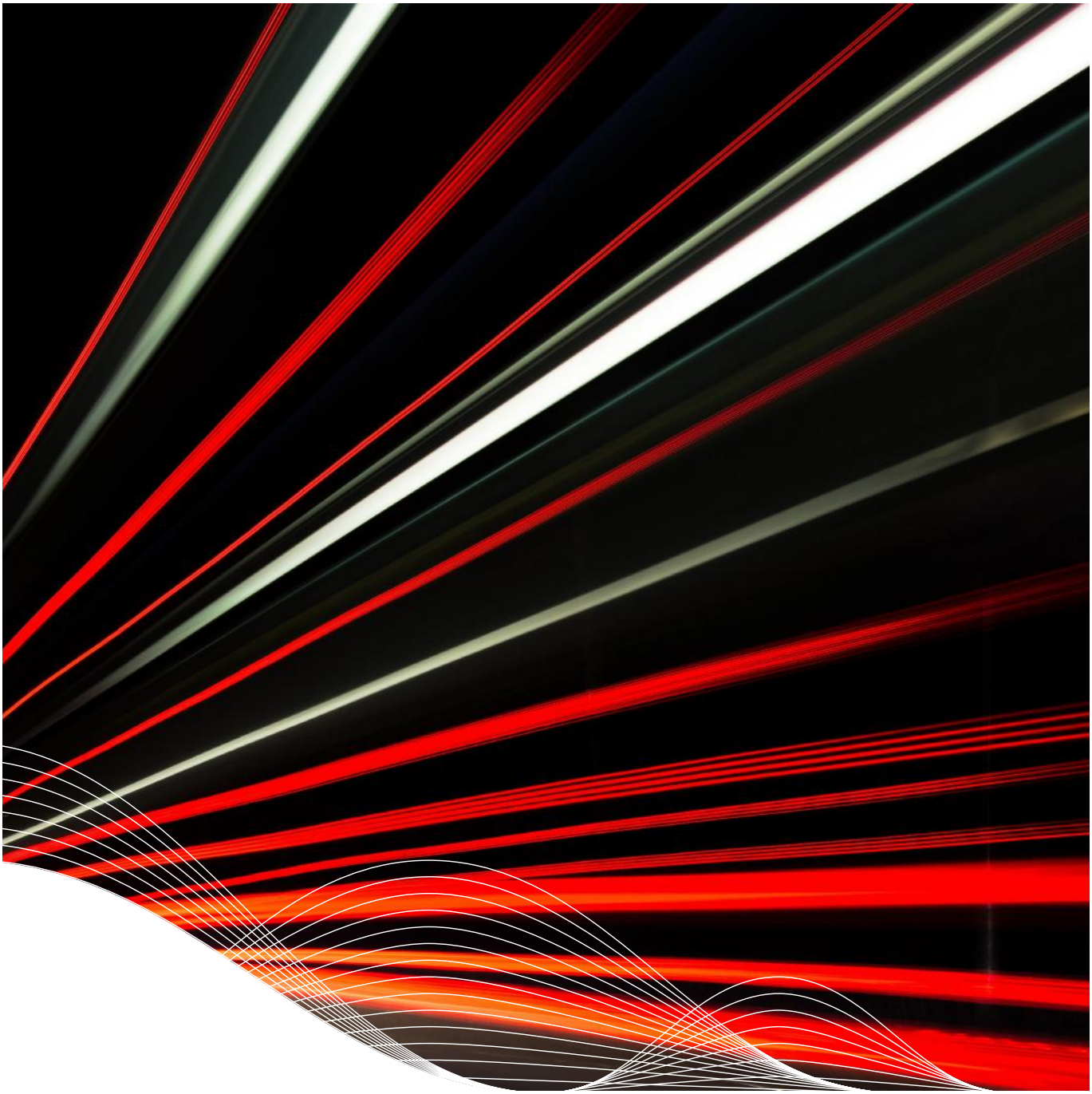


DLA Piper GDPR data breach survey: February 2019

A report produced by DLA Piper's cybersecurity team

DLA PIPER

DLA Piper GDPR data breach survey: February 2019

On 25 May 2018 new data breach notification laws came into force across Europe which fundamentally changed the risk profile for organizations suffering a personal data breach.

Under the EU General Data Protection Regulation - 'GDPR' - personal data breaches which are likely to result in a risk of harm to affected individuals must be notified to data regulators. Where the breach is likely to result in a high risk of harm, affected individuals must also be notified.

Sanctions for failing to comply with the new notification requirements include fines of up to €10 million, or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Although as yet untested in the courts, it is likely that consolidated group revenues will be in the cross-hairs of regulators when they calculate fines.

There is a very short deadline for notification to data protection regulators. Organizations which determine the purposes and means of processing personal data must notify personal data breaches without undue delay and, where feasible, no more than 72 hours after having become aware of it. Where the requirement to notify affected individuals is triggered, these notifications must be made without undue delay.

This report takes a closer look at the number of breaches notified to regulators and the first fines issued under the new GDPR regime for the period from 25 May 2018 to International Data Protection Day on 28 January 2019.

Summary and key findings

In the 8 months since GDPR has applied across Europe, there have been more than 59,000* personal data breaches notified to regulators. These range from minor breaches, such as errant emails sent to the wrong recipient, to major cyber hacks affecting millions of individuals and making front page headlines.

The Netherlands, Germany and the United Kingdom came top of the table with the largest number of data breaches notified to supervisory authorities with approximately 15,400, 12,600 and 10,600 breaches notified respectively.

The countries with the lowest number of breaches notified were Liechtenstein, Iceland and Cyprus with approximately 15, 25 and 35 breaches notified respectively.

When the results are weighted to take into account country population, **the Netherlands leads as the country with the most breaches notified per capita, followed by Ireland and Denmark.** The United Kingdom, Germany and France rank tenth, eleventh and twenty-first respectively while Greece, Italy and Romania have reported the fewest breaches per capita.

Many of the fines imposed over the last year have been under the pre-GDPR regimes, which typically only permitted regulators to impose fines at much lower amounts. **So far 91 reported fines have been imposed under the new GDPR regime.** Not all of the fines imposed relate to personal data breach. The highest GDPR fine imposed to date is €50 million, notably not relating to a personal data breach. This was a decision by the French data protection authority - the CNIL - made against Google in relation to the processing of personal data for advertising purposes without valid authorization.

In Germany, a €20,000 fine was imposed on a company for failing to hash employee passwords, resulting in a security breach. This case is interesting because, in issuing its fine, the German data protection authority (LfDI Baden-Württemberg) appears to have disapplied a provision of the Federal Data Protection Act (BDSG), according to which facts disclosed as part of a breach notification may not be used in proceedings for administrative fines unless the organization concerned consents. In this case LfDI did exactly that - it imposed a fine on the basis of information derived from the breach notification and without the consent of the defendant. The same German data protection authority imposed a €80,000 fine in January 2019 for publishing health data on the internet. German authorities have also reported 62 additional fines.

The remaining fines are relatively low in value, including a €4,800 fine issued in Austria for the operation of an unlawful CCTV system which was deemed excessive for its partial surveillance of a public sidewalk. Cyprus also reported four fines, with a total value of €11,500, and Malta reported a total of 17 fines, a surprisingly large number given the relatively small size of the country. Details of these cases are currently not publicly available.

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 extrapolated the data to cover the full period.
It is also possible that some of the breaches reported relate to the regime pre-dating GDPR.

*Shortly before Data Protection Day (28 January 2019) the European Commission reported 41,502 data breach notifications for the same period. However, these results were based only on the voluntary contributions of 21 (out of 28 EU Member States) data protection regulators. Based on our own research covering 23 of the 28 EU Member States, together with figures for Norway, Iceland and Lichtenstein (the three additional European Economic Area Member States), we calculate that there have been 59,430 reported data breaches over the same period across Europe. Notably, official figures reported by the Dutch data protection supervisory authority on 29 January 2019 reported approximately 15,400 data breach notifications for the same period just for the Netherlands. The breach notification figures in our report are nevertheless best approximations as it is possible that some of the breach notifications reported relate to the regime pre-dating GDPR. We have also extrapolated some data points which did not neatly match the eight month period from 25 May 2018 to 28 January 2019.

Comment

It is clear from the data that many organizations have heeded the new breach notification rules, no doubt in part due to concerns about the high sanctions for not notifying, leading to more than 59,000 personal data breaches being notified across Europe in the first 8 months since 25 May 2018. Sweeping data breaches under the carpet has become a very high-risk strategy under GDPR.

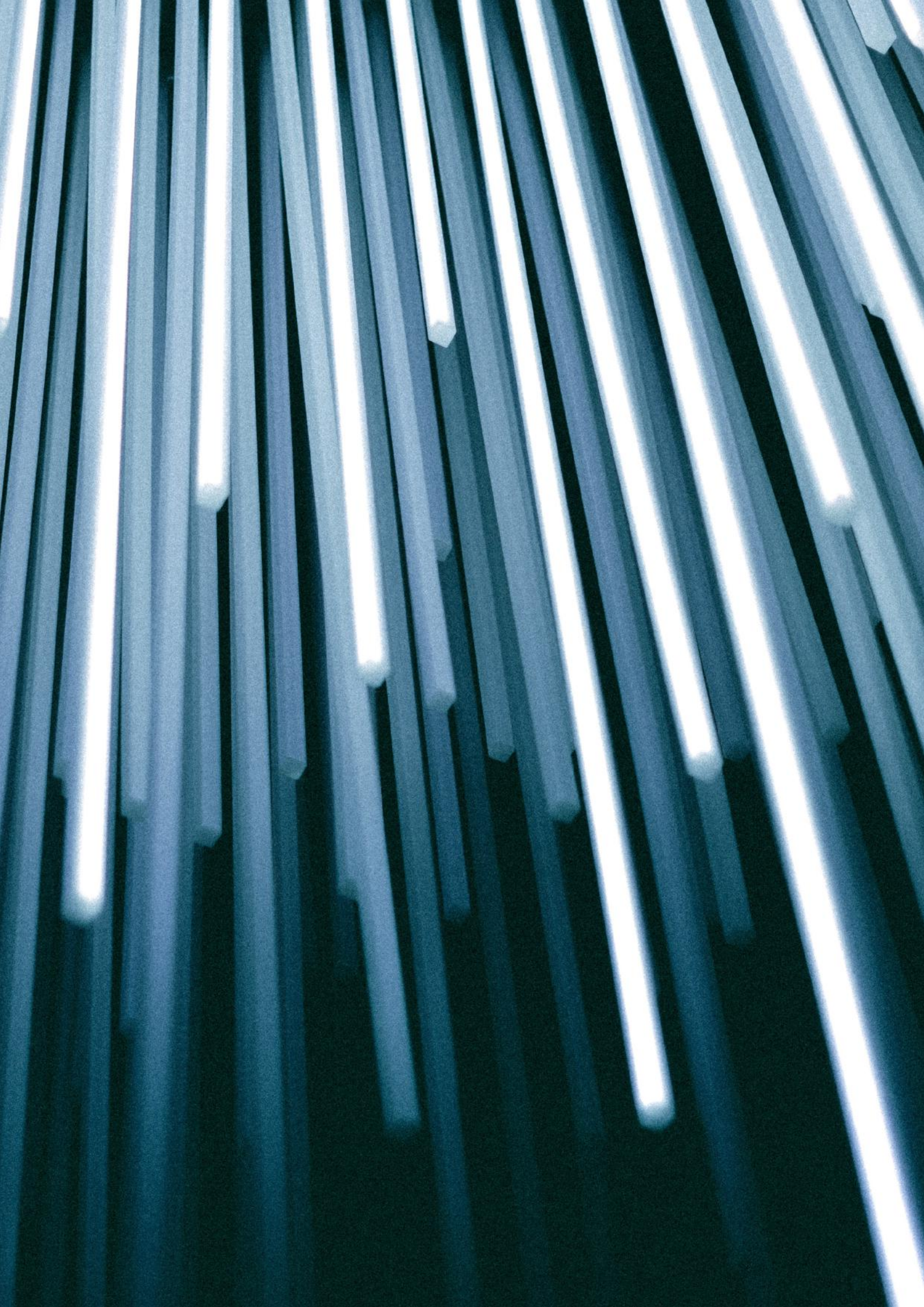
Regulators are stretched and have a large backlog of notified breaches in their inboxes. Inevitably the larger headline grabbing breaches have taken priority when allocating resources, so many organizations are still waiting to hear from regulators whether any action will be taken against them in relation to the breaches they have notified.

The weighted rankings are also revealing. In particular Italy has so far had very few breach notifications relative to its large population which illustrates that notification practice and culture varies significantly among Member States. It is important to note that this report focuses on reported data breaches only.

It is still very early days for GDPR enforcement with only a handful of fines reported across the EU. With the exception of the recent €50 million fine imposed on Google, so far the level of fines have been low, certainly when compared to the maximum fines regulators now have the power to impose. However, we anticipate that 2019 will see more fines for tens and potentially even hundreds of millions of Euros as regulators deal with the backlog of GDPR data breach notifications. It is likely that regulators and courts will look to EU competition law and jurisprudence for inspiration when calculating GDPR fines and some regulators have already said they will do so. Competition lawyers are not known to shy away from imposing hefty fines and have imposed some eye-catching multi-billion Euro fines recently on large tech companies.

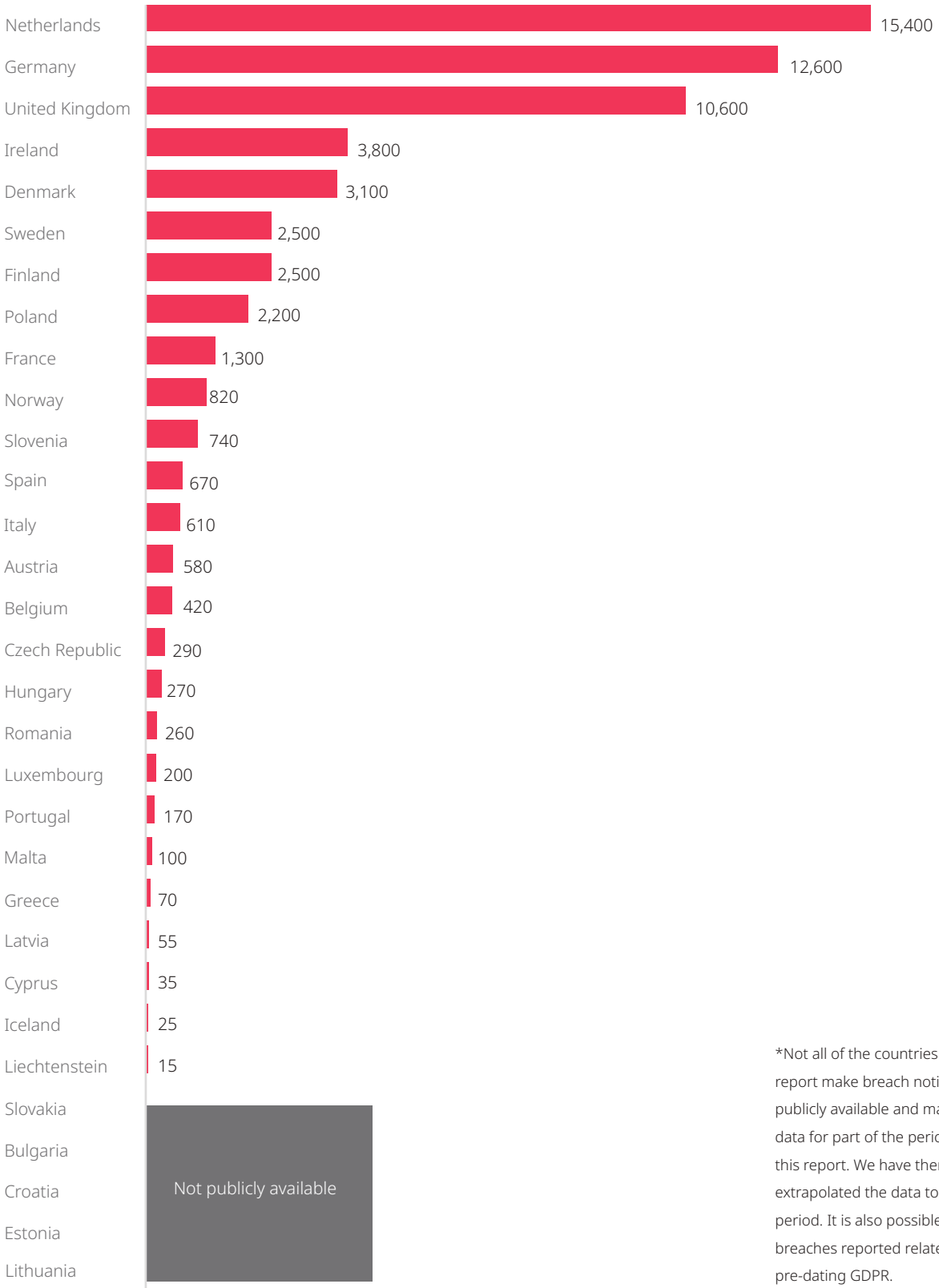
That said, this is yet another area where there are important open legal questions under GDPR. Some legal commentators in Germany argue that applying EU competition law principles to calculate GDPR fines would violate the principles of legality and proportionality of criminal offences and penalties under the European Charter of Fundamental Rights and therefore local German procedural rules should be applied to calculate GDPR fines, resulting in much lower fines being applied. We anticipate that there will be early test cases on this point as the regulators trial the limits of their new powers.

This publication has been prepared by DLA Piper. We are also grateful to Batliner Wagner Batliner Attorneys at Law Ltd., Glinska & Mišković Ltd., Kambourov & Partners, Kyriakides Georgopoulos Law Firm, Logos Legal Services, Mamo TCV Associates, Pamboridis LLC and Sorainen for their contributions in relation to Liechtenstein, Croatia, Bulgaria, Greece, Iceland, Malta, Cyprus and Estonia respectively.



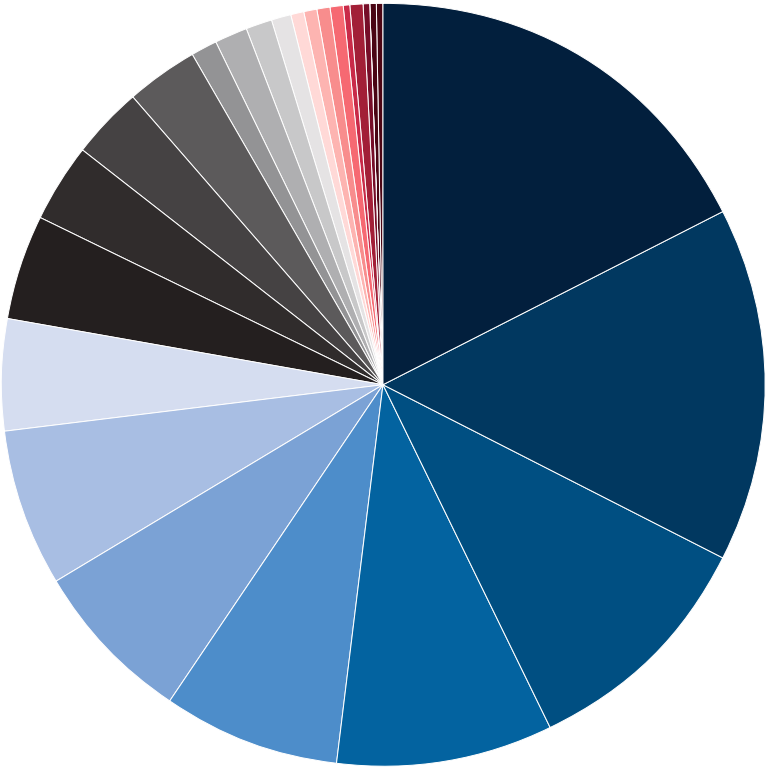
Report

NUMBER OF DATA BREACHES NOTIFIED FROM 25 MAY 2018 TO 28 JANUARY 2019*



*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 extrapolated the data to cover the full period. It is also possible that some of the breaches reported relate to the regime pre-dating GDPR.

PER CAPITA COUNTRY RANKING OF BREACH NOTIFICATIONS*	NUMBER OF DATA BREACHES PER 100,000 PEOPLE
Netherlands	89.8
Ireland	74.9
Denmark	53.3
Finland	45.1
Liechtenstein	38.9
Slovenia	35.2
Luxembourg	33
Sweden	24.9
Malta	22.3
United Kingdom	16.3
Germany	15.6
Norway	15.2
Iceland	7.2
Austria	6.6
Poland	5.7
Belgium	3.6
Cyprus	2.8
Latvia	2.8
Hungary	2.7
Czech Republic	2.7
France	1.9
Portugal	1.6
Spain	1.3
Romania	1.2
Italy	0.9
Greece	0.6



*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 (last updated July 2018 est.).