European data regulators issued EUR1.1 billion in GDPR fines – a sevenfold year on year increase - survey by DLA Piper

Nearly EUR1.1bn of fines have been imposed in 2021 for a wide range of infringements of Europe's General Data Protection Regulation. This represents a 594% year on year increase in fines imposed since 28 January 2021 compared to EUR158.5m during the same period last year (28 january 2020 – 27 january 2021), according to international law firm DLA Piper. The figure is taken from the law firm's latest annual ***General Data Protection Regulation (GDPR) fines and data breach survey*** *of the 27 European Union Member States plus the UK, Norway, Iceland and Liechtenstein.*

Luxembourg, Ireland and France top the rankings for the highest individual fines (EUR746m; EUR225m and EUR50m respectively). Luxembourg and Ireland have each imposed record-breaking fines moving them from the bottom to the top of the league tables.

The growth of breach notifications has continued with an 8% increase from last year's average of 331 notifications per day to 356 this year and more than 130,000 personal data breaches notified in aggregate since 28 January 2021.

Weighting the results against country populations, the Netherlands takes pole position this year ahead of Liechtenstein and Denmark with 151, 136 and 131 breach notifications per 100,000 people respectively. Croatia, the Czech Republic and Greece reported the fewest number of breach notifications per capita since 28 January 2021.

While the increase in fines may be significant, the judgment of Europe's highest court in *Data Protection Commissioner* v *Facebook Ireland Limited, Maximillian Schrems* in July 2020 known as "*Schrems II*" continues to be the top data protection compliance challenge for many organisations caught by GDPR. The judgment and Chapter V of GDPR impose strict limitations on the transfer of personal data from Europe and the UK to "third countries" with data exporters risking suspension orders, fines and claims for compensation for failing to meet these new requirements. The judgment requires organisations exporting personal data from Europe and the UK to third countries to carry out comprehensive mapping of those transfers and detailed assessments of the legal and practical risks of interception by public authorities in the countries where importers are located, greatly increasing the compliance burden on data exporters and importers.

According to the survey findings the *Schrems II* judgment doesn't just create a risk of fines and claims for compensation, it also threatens service interruption in the event data transfers are suspended, with serious implications for business continuity.

Irina Macovei, Counsel DLA Piper Romania, comments on the interpretation of the results of this survey: *“The dramatic increase in the number of fines and the considerable values □ □ should be understood as warnings addressed to both data controllers and their processors, and transposed into increased attention to this area. It is obvious that the requirements of the supervisory authorities are on the rise and it could be argued that there is already sufficient information, resources and time for compliance”*.

The local approach is aimed, in particular, at raising awareness in order to comply with legal provisions, as **Andrei Stoica**, Managing Associate DLA Piper Romania, points out: *“In Romania, the value of fines is, at least for the time being, rather low compared to other Member States, because we still benefit from the supervisory authority's approach aimed at raising awareness and educating organizations and data subjects. This attitude is obvious, if we compare the relatively large number of sanctions, which places us above most of the European countries, to the unimpressive value of the fines.”*

"It should be noted that, in addition to fines, there are other sanctions that have been applied by ANSPDCP, such as warnings", says **Irina Macovei**. *"The reputational impact should not be overlooked either, as the sanctions imposed are public."*

“ANSPDCP also ordered corrective measures (cessation of non-compliant practices, compliance with the requirements of personal data protection legislation, observance of the rights of data subjects, implementation of appropriate technical and organizational measures to ensure an adequate level of security, training staff on the measures taken by the controller, reviewing and updating the working procedures regarding the protection of personal data etc.). These corrective measures can in some cases be more expensive than the fines themselves", adds **Andrei Stoica**.