Bloomberg Law®

Reproduced with permission from Bloomberg Law Insights. First published online on May 1, 2019: https://news.bloomberglaw.com/us-law-week/insight-a-slap-on-the-wrist-or-show-of-force-gdpr-fines-reveal-need-for-eu-penalty-guidelines. 

# INSIGHT: A SLAP ON THE WRIST OR SHOW OF FORCE—GDPR FINES REVEAL NEED FOR EU PENALTY GUIDELINES

*The EU's data protection law gives authorities discretionary power for setting penalties, but it doesn't say how penalties should be determined. A Morrison & Foerster head privacy attorney and an analyst in Brussels say the first year of GDPR fines shows the need for specific guidelines for consistent enforcement.*

By Alex van der Wolk and Karine e Silva

Fines imposed under the European Union's General Data Protection Regulation are capturing widespread attention—from the first minor sanction imposed by the Austrian Data Protection Authority (DPA) to the multi-million dollar fine levied by the DPA against Google.

*Alex van der Wolk, global co-chair of Morrison & Foerster's Privacy and Data Security Group, in Brussels, specializes in data protection information/communications technology law. He advises global companies on data protection strategy and compliance governing all aspects of information management.*

*Karine e Silva is a privacy analyst with Morrison & Foerster in Brussels. She is also a Ph.D. candidate at Tilburg University.*

Under the GDPR, European DPAs can impose fines of up to €20 million ($22.6 million) or 4 percent of annual revenue of a company. And although GDPR awards DPAs discretionary power for penalty setting, it does not indicate how penalties in any given case should be determined.

This lack of direction undercuts consistency and predictability. Indeed, the first year of GDPR enforcement has been accompanied by a perception that DPAs are calculating administrative fines individually and unsystematically.

## Penalty System

GDPR Article 83 introduces two bands of penalty maximums: €10 million ($11.3 million) or 2 percent of revenue and €20 million ($22.6 million) or 4 percent, where the maximums operate as a ceiling after the specifics of each case have been weighed.

To that end, Article 83(2) introduces a list of factors that DPAs should consider when determining fines, each of which can operate as a mitigating or aggravating factor to the ultimate penalty amount.

In its guidance, the European Data Protection Board suggests DPAs take the entire Article 83(2) into consideration, which includes (among others) the nature and duration of the infringement, any intent or negligence, actions to mitigate damages, and cooperation with the DPA.

### First Year of Fines

In recent enforcement actions, DPAs have applied Article 83(2).

In January 2019, the CNIL imposed a €50 million ($57 million) fine on Google for alleged GDPR violations of the transparency, notice, and consent requirements. The CNIL stated generally that it considered all criteria of Article 83(2), while mentioning the aggravating circumstances, namely, the pervasive nature of the processing, the ongoing violation, the high number of individuals involved, and the fact that Google derived benefits from the processing.

When the Portuguese DPA (CNPD) imposed a €400,000 ($450,000) fine on a hospital in October 2018 regarding the administration of its patient database, it broke the amount down as per three separate GDPR violations. The CNPD considered the specifics of the case and found the following circumstances to have aggravated the violation: the nature of the data, the means by which the DPA became aware of the violation, and the hospital's failure to implement previous recommendations.

At the time of writing, the latest GDPR fine was issued in Poland: a €220,000 ($250,000) fine against data brokers who violated their obligation to inform under Article 14 GDPR. The DPA found that the company had failed to notify over 6.6 million people whose data had been obtained from publicly available sources, a violation subject to the second band of up to €20 million ($22.6 million) or 4 percent of revenue.

Remarkably, in none of these cases the DPAs provided any reasoning as to how they determined the actual penalty amount. In particular, none of them substantiated how the factors of Art. 83(2) influenced the overall calculation or disclosed any basic starting amount to which those factors were applied.

Even where DPAs found that multiple violations had taken place, they either did not disclose how each violation contributed to the total penalty amount or did not substantiate how each amount per violation was reached. The overall lack of transparency about a rational method used by the DPAs goes against the principles of transparency, accountability, and consistency in administrative decisions.

### Penalty Guidelines

In other compliance areas such as antitrust, it is well established for regulators to issue penalty guidelines. Like the GDPR, European antitrust law allows for fines as a percentage relative to a company's total worldwide annual revenue.

However, the European Commission (EC) has issued guidelines outlining how it will determine final penalties through a three-step methodology. First, the EC determines the basic amount based on the value of goods or services affected by the antitrust infringement. Second, it applies upward or downward adjustments through mitigating and aggravating factors. Finally, the EC determines whether the resulting fine should be the provided maximum. While the reference to value of goods or services would not be applicable in a GDPR context, the EC's methodology is a useful guide.

In fact, similar methodology has been developed by the Dutch DPA. In its penalty guidelines published in March 2019, GDPR obligations are divided into a total of four categories. For each category, a band and a basic amount. Each violation is then assessed by determining the basic amount for the respective category to which the aggravating and mitigating

factors of Article 83(2) are applied. The final penalty within each category should not exceed the categories' upper or lower boundaries.

In exceptional cases, the DPA can issue a fine outside a category range (if that would be more fitting), as long as this is within the maximum provided by GDPR. Therefore, while the Dutch approach still allows for discretion to issue penalties outside the defined categories, the guidelines do provide for a more structured and predictable approach to set fines.

The first year of GDPR enforcement has shown a number of things. First, that DPAs do indeed intend to use their fining power for GDPR violations. But also that the GDPR itself does not provide for a structure and system to determine specific penalties in any given case.

In fact, the first enforcement actions suggest an unsystematic and opaque approach to GDPR fines. Significant discrepancies in fines can have a negative impact on the goal of harmonization promoted in the GDPR and have a detrimental effect on corrective measures.

While some DPAs are making efforts to apply penalty guidelines, specific guidelines issued at European Union level are necessary to achieve consistency in GDPR application among Member States.

*This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.*