DIGITALEUROPE

27 JUNE 2022

# Harmonising enforcement in methods to calculate administrative fines

## Executive summary

Fines are one of several types of sanctions under the General Data Protection Regulation (GDPR),[1] and their effectiveness particularly relies on harmonisation. Each decision to fine has an economic impact, with the potential to reverberate across the EU's single market. A strong common methodology behind the calculation of fines could help level the playing field, provide legal certainty and strengthen compliance.

For this reason, while we welcome the European Data Protection Board's (EDPB) efforts to ensure a common orientation for the calculation of administrative fines,[2] we note a lack clarity in several key areas of the draft Guidelines.

### We particularly encourage the EDPB to:

- Incentivise, rather than dismiss, actions taken by controllers and processors to mitigate the risk of damage to individuals, as well as actions to comply with Arts 25 and 32 GDPR;
- Transparently define the starting point for the calculation of administrative fines, and notably the scope of any principles which may apply;
- Further specify principles which find their roots in competition law, to ensure a consistent application alongside the GDPR; and
- Avoid divergence in the decisions made by different supervisory authorities, which could arise from a lack of clarity in the Guidelines.

[1] Regulation (EU) 2016/679.

[2] Draft Guidelines 04/2022 on the calculation of administrative fines under the GDPR, available at https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf.

**DIGITALEUROPE**
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

# Table of contents

# Mitigating and aggravating circumstances

Guidance on what may be considered as a mitigating or, on the contrary, an aggravating circumstance is of particular importance, as it enables controllers and processors to understand what is expected and how best to comply.

## Actions to mitigate damage

With regard to the actions that can be taken to mitigate damage suffered by data subjects[3], we believe that spontaneous measures implemented by the controller or processor should be taken into account, whether they take place before or after an investigation becomes known to them.

In some cases for instance, the controller or processor is not informed of an issue before the investigation begins and therefore cannot take prior mitigating measures. However, once the investigation does begin, particular effort can be made to quickly react to exchanges with the supervisory authority (SA).

Therefore, priority should be given to finding effective measures that can protect the individuals concerned. Solutions to mitigate damage can arise at different stages of the investigations and should be encouraged rather than dismissed.

Focusing on the effectiveness of measures is of particular importance, as according to the draft Guidelines, their analysis is a 'first step' for SAs in determining aggravating or mitigating circumstances.

## Going 'above and beyond' legal obligations

In describing the controller's and processor's degree of responsibility, the draft Guidelines go a step further than previous guidance[4], which mentions what the controller is 'expected to do'. The current WP29 Guidelines place the degree of responsibility in the context of the 'nature, the purposes or the size of the processing seen in the light of the obligations imposed on [controllers and processors] by the Regulation', a context which is not accounted for in the draft Guidelines.

By contrast, the draft EDPB Guidelines restrict responsibility to 'where the controller or processor has gone above and beyond the obligations imposed on 'them' by the GDPR'. Asking the controller or processor to go 'above and beyond' what is required by the law is excessive. Instead, the final Guidelines could be replaced with simply state that it is possible that compliance with Arts 25 and 32 GDPR can exceptionally constitute a mitigating circumstance. This would avoid subjective approaches and limit divergence in decisions taken by different SAs.

---

[3] Para. 77 of the draft Guidelines.

[4] See p. 13, WP29 *Guidelines on on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, WP 253.

## Defining the starting point for the calculation

We welcome the analysis made of Member States' traditions of rules on concurrences in CJEU case-law, and the draft Guidelines' effort to clarify which of those principles could be relied upon. However, the different scopes of application for each principle should be clarified.

### Scope of the speciality principle

The Guidelines should expand on how far infringements must overlap in order for a concurrence of offences may be found.[5] This would be particularly important as the principle of unity of action also relies on the definition of the scope of the speciality principle. Understanding what principles the methodology to calculate the fine is based on would further allow the controller or processor to understand the basis of a fine. If SAs follow the listed principles harmoniously, decisions will automatically use a similar logic.

### Seriousness and gravity of an infringement

The draft Guidelines refer to the amount of data regarding each data subject as a criterion to determine how serious an infringement is.[6] However, the preceding paragraph discusses the categories of personal data affected, based on Art. 83(2) GDPR, not the amount of data. We find both paragraphs to be contradictory in the way they are presently phrased.

When assessing the gravity of the infringement, Art. 83(2)(a) does take into account the scope of processing but does not refer to how central the processing is to the controller's or the processor's core activities.[7] The fact that there are circumstances under which the processing is not central but does impact the evaluation shows that this element is not of strong relevance. It therefore arguably brings uncertainty as to the obligation for controllers and processors to pay more attention to the data which may be considered central to their activities. The draft Guidelines do not provide an indication as to what may be considered a 'core activity' or which data is 'central'.

### Duration

While weight should be given to the duration of the infringement, Art. 83(2)(a) does not indicate that an infringement is more serious because it began under the previous regulatory framework.

The sentence 'a given conduct might have been illicit also within the previous regulatory framework, thus adding an additional element to assess the gravity of the

[5] Para. 35 of the draft Guidelines.

[6] Para. 58, ibid.

[7] Para. 54, ibid.

infringement.' adds a level of complexity to the element of duration, which can be found neither in Art; 83(2)(a), nor in the GDPR's recitals. To take into account actions covered by a different legal framework would be contrary to the principle of non-retroactive application of law.

## Elements from competition law

In determining the legal maximum for a fine, several concepts in the draft Guidelines reflect competition law. Two examples are in the definition of an undertaking or the application of the Akzo presumption. Concepts from competition law might apply differently in the enforcement of the GDPR and would require additional clarity.

### Definition of an undertaking

The draft Guidelines base the definition of an undertaking on the GDPR recitals, which themselves refer to Arts. 101 and 102 TFEU.[8] Although the draft Guidelines seem to focus on consistency rather than cooperation, referencing the one-stop-shop in fining undertakings would clarify the scope of these definitions under data protection law. This should notably ensure that fines are not imposed directly on establishments present in the territory of an SA, without the case being referred to the lead SA appointed under Art. 60 GDPR.

### The Akzo presumption

The draft Guidelines underline that the Akzo presumption is not absolute, in that it can be rebutted. Such evidence must widely relate to 'organizational, economic and legal links between the subsidiary and its parent company', without further detail. Since the burden is on the controller or processor to reverse the Akzo presumption, the Guidelines should further explain the circumstances under which a rebuttal can be made, especially for undertakings with sometimes complex structures.

## Proportionality and deterrence

The proportionality of a fine and the proof of value loss should take into account the reputational damage which a company may suffer from the issuing of a fine. Such damage can have a lasting effect and could contribute to jeopardising the economic

[8] Recital 150 GDPR.

viability of an undertaking. The influence decisions can have on businesses' profitability should not be ignored.[9]

Proportionality should allow the gravity of the fine to reflect the gravity of the infringement. While the size of the organisation can be an element of the decision, it should not take precedence. The Guidelines might otherwise risk emphasising the notion that fines under the GDPR are only a risk to a small number of large corporations.

Finally, the possibility for SAs to increase the fine 'if they do not consider the amount to be dissuasive' should be clarified. The draft Guidelines aim to find a common methodology to calculate administrative fines. Concluding a precise and structured analysis with the argument that a deterrence multiplier can be justified, without providing more detail as to the circumstances for such justification, would defeat the very purpose of the Guidelines.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

**Director for Infrastructure, Privacy and Security Policy**

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Béatrice Ericson

**Officer for Privacy and Security Policy**

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

[9] See also pp. 7-8 of our position paper *Almost two years of GDPR: celebrating and improving the application of Europe's data protection framework*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/01/Position-paper-on-GDPRreview.pdf.

## About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

# DIGITALEUROPE Membership

### Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Banco Santander, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

### National Trade Associations

**Austria:** IOÖ
**Belgium:** AGORIA
**Croatia:** Croatian Chamber of Economy
**Cyprus:** CITEA
**Czech Republic:** AAVIT
**Denmark:** DI Digital, IT BRANCHEN, Dansk Erhverv
**Estonia:** ITL
**Finland:** TIF
**France:** AFNUM, SECIMAVI, numeum
**Germany:** bitkom, ZVEI
**Greece:** SEPE
**Hungary:** IVSZ
**Ireland:** Technology Ireland
**Italy:** Anitec-Assinform
**Lithuania:** Infobalt
**Luxembourg:** APSI
**Moldova:** ATIC
**Netherlands:** NLdigital, FIAR
**Norway:** Abelia
**Poland:** KIGEIT, PIIT, ZIPSEE
**Portugal:** AGEFE
**Romania:** ANIS
**Slovakia:** ITAS
**Slovenia:** ICT Association of Slovenia at CCIS
**Spain:** Adigital, AMETIC
**Sweden:** TechSverige, Teknikföretagen
**Switzerland:** SWICO
**Turkey:** Digital Turkey Platform, ECID
**Ukraine:** IT Ukraine
**United Kingdom:** techUK