CEN – European Committee for Standardization
CENELEC – European Committee for Electrotechnical Standardization

CEN Identification number in the EC register: 63623305522-13

CENELEC Identification number in the EC register: 58258552517-56

FEEDBACK OF CEN-CENELEC JTC13/WG5 Consultation Task Force on EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 1.0

27 June 2022

TABLE OF CONTENTS

Introduction

CEN and CENELEC are two of the three European Standardization Organizations (ESOs) whose main common objective is to remove trade barriers for European industry and consumers. The joint mission of CEN and CENELEC is to provide European Standards to foster the European economy in global trading, the welfare of European citizens and the environment.

CEN/CLC JTC13 is a joint technical committee the scope of which is to develop standards about Cybersecurity and Data protection to address at best the European needs, including in support of the European regulations. WG5 is the competent Working Group " Data Protection, Privacy and Identity Management"?

Standards are essential tools to help market stakeholders in their practical implementation in the domains of cybersecurity and data protection and for supporting the demonstration of compliance to the EU regulatory obligations, including the ones established by the Regulation 2016/679 (GDPR).

In this framework, the "CEN/CLC/JTC13/WG5 Consultation Task Force" (hereinafter ''the Consultation Task Force'') – is submitting the following document as a contribution to the public consultation on the EDPB "Guidelines 04/2022 on the calculation of administrative fines under the GDPR".

The presence and work of the Consultation Task Force aligns with the CEN/CLC JTC 13's strategic business plan and the defined objectives therein, which include JTC 13 being identified as a strategic partner of institutions, agencies and bodies within the EU system being involved in the Cybersecurity and Privacy policy and law making and a strategic partner of EU Member States' national administrations and bodies/entities involved in the Cybersecurity & Privacy policy and law making.

The scope of the Consultation Task Force is to participate in public and private consultations for data protection, privacy and identity management issues initiated, amongst others, by institutions, agencies, and bodies within the EU system, being involved in the Cybersecurity & Privacy policy and law making or initiated by national bodies and entities such as Member States' national supervisory authorities.

For any clarification or questions regarding this feedback, please address this by sending an email to the email addresses:

Consultations Group Coordinator: maria@privacyminders.com
WG5 Convener: a.guarino@stagcyber.eu
JTC13 Secretariat: martin.uhlherr@din.de

Chapter 2-Methodology for calculating the amount of the fine (p.7,8)

Infringements with fixed amounts (section 2.3, p. 8)

The EDPB states that the Supervisory Authorities (SAs) may consider establishing fixed amounts, at their own discretion, for certain infringements.

On the one hand, the SAs appear to lack statutory power to establish fixed amounts for certain infringements.

Article 84.1 of the GDPR, from which the EDPB, may have considered that the SAs derive such power, states, however, that MS shall lay down the rules **on other penalties** applicable to infringements which are not subject to administrative fines pursuant to article 83.

We would argue, nevertheless, that the encouragement of SAs to consider establishing fixed amounts violates the principle of accountability and the principle of proportionality in setting administrative fines and is inconsistent with:

(a) GDPR's requirement for each individual case to be subject to an effective, proportionate and dissuasive administrative fine (art. 83(1) of the GDPR);
(b) the requirement to decide on the amount of the administrative fine in each individual case based on specific criteria (art. 83(2) of the GDPR).

Chapter 3-Concurrent infringements and the application of Article 83(3) of the GDPR

Multiple infringements for one sanctionable conduct

Concurrence of Offences (section 3.1.1, p. 12, 13)

Principle of Speciality

In that case, the application of one provision precludes or subsumes the applicability of the other.

The EDPB considers this to take place by virtue of the principle of specialty, where the objectives pursued by the concerned infringement are congruent in the individual case. We would welcome a specific example by EDPB of such cases.

The only example provided by EDPB is for the case where the objectives of the provisions are not congruent i.e., the data protection principles in Article 5 of the GDPR versus the provisions that are a concretization of such principle.

The Data Protection Commission (DPC) with its decision against WhatsApp IE of 20.08.2021 issued a separate fine for the infringement of the overarching transparency principle and separate fines for infringing art. 13 and 14 information obligations (and other specific transparency obligations) towards users and non-users. It was stated by the DPC that it is possible to find an infringement of transparency obligations independently from the infringement of transparency principle in light of the gravity and the overarching nature and impact of the infringements. It stems from the above reasoning that the DPC does not consider all violations of GDPR provisions that concretize data protection principles to be simultaneously finable violations of such principles.

EDPB's obvious clarification that GDPR provisions may be a concretization of a data protection principle opens the pathway for all infringements of GDPR provisions that emanate from data protection principles to simultaneously be rendered infringements of the corresponding data protection principles.

The guidelines in discussion do not indicate EDPB's stance on whether, depending on the circumstances of the case, a violation of a GDPR provision that concretizes a data protection principle, may or may not be a finable violation of such principle.

Lastly, we would invite EDPB to provide examples of congruency of objectives of GDPR provisions and more examples of congruency of objectives of GDPR provisions.

Principle of subsidiarity and principle of consumption (P. 13)

We would invite the EDPB to provide examples.

Unity of Action or Ideal Concurrence (section 3.1.2, p. 13, 14,15)

This is the case where one conduct is caught by several statutory provisions, but one provision is neither precluded nor subsumed by the applicability of the other, because they do not fall in the scope of the principles of specialty, subsidiary or consumption and mostly pursue different objectives.

Art. 83(3) of the GDPR: If a controller or processor **intentionally or negligently**, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

The benefit a controller or processor enjoys from art. 83(3) arises where the infringement is either intentional or negligent. We understand that the reference to intentional or negligent infringements reflects the intent of the legislator to cover all infringements of the GDPR for the same or linked processing operations, without any exceptions. Therefore, we would invite the EDPB to state that ‘’negligence’’ shall be interpreted broadly in a way that it encompasses acts or omissions of the controller or processor that may not be negligent per se i.e., purely negligent but also those that may be the result of carelessness or, even, those that may not be intentional but are not negligent either. This may be the case of a controller or processor that exercised diligence and care to safeguard that the processing operations comply to the GDPR, however the interpretation or the application of the legislation or guidelines was considered by the supervisory authorities to be inappropriate or misguided.

Otherwise, reference to intentional or negligent infringements may be considered a restriction imposed by the GDPR as to the applicability of art. 83(3), so as to exclude infringements that are not intentional or negligent, whereas this was clearly not the intent of the legislator.

Chapter 4-Starting point for calculation

The EDPB considers three elements to form the starting point for further calculation:

(a) The categorisation of infringements by nature under Articles 83(4)-(6) of the GDPR;
(b) The seriousness of the infringement pursuant to Article 83(2) GDPR, considering the criteria in article 83(2)a, b and g of the GDPR;
(c) The turnover of the undertaking.

The categorisation of infringements under Articles 83(4)-(6) GDPR (p.16)

The EDPB invites the SAs, prior to assessing the seriousness of the infringement in each individual case, to consider whether the infringement is punishable under art. 83(4) or articles 83(5) and (6), as this signals, according to the EDPB, a first indication of the severity of the infringement.

The categorisation of the infringement together with the assessment of the criteria mentioned in article 83(2)a, b and g of the GDPR will lead, according to EDPB, to the classification of the overall seriousness of the infringement as low, medium or high and the establishment of the starting amount of further calculation (0-10% of the applicable legal maximum for low level of seriousness, 10-20% for medium level and 20 to 100% for high level).

In our opinion, considering the category of the infringement for establishing the starting amount of further calculation is a misplaced approach.

The choice of the legislator to attribute higher legal maximums for infringements of certain type indeed signals that these infringements may have the tendency or potential to be more serious infringements, in terms of their nature and gravity, as they relate to fundamental provisions of the GDPR. The legislator has acknowledged and conceived this prospect, granting to the SAs the power to grant higher administrative fines, by virtue of a higher legal maximum.

We note, however, that the actual level of seriousness of an infringement and the level of damage (material or non-material) that is capable of inflicting on individuals is not necessarily lower for infringements under art. 83(4) of the GDPR in comparison to infringements under art. 83(5) of the GDPR.

For example, infringements relating to security of processing are listed in art. 83(4) and, therefore enjoy a lower legal maximum, however, such infringements can cause significant and grave damages to a significant number of individuals and society which may be greater than the damage inflicted when the controller omits to include in its privacy notice information on data retention, an infringement covered under art. 83(5) of the GDPR.

Intentional or negligent character of the infringement (section 4.2.2, p.56)

The EDPB solely discusses the intentional and negligent stance of the controller of processor leading down to the infringement, with negligence being considered by the EDPB to exist where the controller of processor breached the duty of care which is required by the law. It does not address, however, situations which do not fall on either side of the spectrum, but rather showcase the controller's or processor's goth faith effort, driven by the principle of accountability, to interpret and apply the legislation in a way that does not coincide with the SA's interpretation and approach, during the investigation, audit, and assessment process.

We would recommend that situations capturing the controller's or processor's good faith effort to receive, mutatis mudandis, treatment which is more favourable in comparison to negligent infringements which are the result of breach of duty of care, especially in cases of indeterminacy, unpredictability, inconsistent and vague interpretations across Member States and, generally, cases which require from the controller and processor to exercise a high level of discretion and judgment (e.g. to comply with Data Protection by Design and by Default obligations).

The turnover of the undertaking (section 4.3, p.22-24)

The EDPB considers that it is fair to consider the size of the undertaking in the starting points and take into account its turnover, significantly increasing or decreasing the amount of the fine, with a view to imposing an effective, dissuasive and proportionate fine. As a general rule, the EDPB states, the higher the turnover of the undertaking within its applicable tier, the higher the starting amount is likely to be.

This has the effect of utilizing the turnover of an undertaking not only for determining the maximum amount, but for the calculation of the fine itself.

We agree with the turnover being an element to evaluate while considering establishing the starting point, but we are of the view that consideration should be given on whether looking on turnover to establish the starting point of the fine, may lead, in some cases, to fines that are disproportionate. For example, some GDPR violations may not be relevant to the core business of the violator who may have not generated any direct profit from the personal data processing operations, or the violations may have not caused measurable economic harm to individuals. Article 83(2)k of the GDPR refers to financial benefits gained, or losses avoided directly or indirectly from the infringement as an aggravating or mitigating factor. The level of damage inflicted on the individuals and the number of data subjects affected appears to be a more reliable choice.

Chapter 5-Aggravating and mitigating circumstances

Adherence to approved codes of conduct or approved certification mechanisms (section 5.8, p.29)

The EDPB clarifies that if failure to comply with the codes of conduct or certification is directly relevant to the infringement, the SA may consider this an aggravating circumstance.

We assume that the EDPB refers to the failure of the organisation to comply with codes of conduct or certification, from which an analogous infringement of a GDPR provision can be determined. Should our understanding be incorrect, we would welcome EDPB's clarification in the finalised guidelines. If our understanding is correct, we would like to express our strong disagreement with the stance adopted by the EDPB in this regard. The controllers or processors should be encouraged and not prevented from adhering to codes of conduct or certification. The risk that the monitoring of compliance with a code of conduct and the assessment leading to the certification being issued and maintained entails is by itself a preventative factor against aiming at adhering to codes of conduct or certifications. For example, a certification may be withdrawn because the controller or processor no longer complies with a certification criterion, and this may trigger the investigation and audit process by the competent SA. The mere fact that the infringement identified is related to any certification criteria which the controller or processor no longer complies with shall not, under any circumstances, be an aggravating factor. The choice of the Controller and Processor to expose themselves to the scrutiny of the monitoring body, certification body and supervisory authority should not place them at such disadvantageous state.

CEN/CLC/JTC13/WG5 considers that GDPR Certification can promote and enhance the accountability of organisations and at the same time assist them with their compliance efforts.

For this reason, the JTC13/WG5, in order to provide support to Certification Schemes under development and/or the development of Certification Schemes is developing:

(a) JT013037 Privacy Information Management System per EN/ISO/IEC 27701 – refinements in a European context" specifications which can be used by competent bodies (CABs, SAs) to specify data protection certification mechanisms as per GDPR article 42 in order to assess the conformity of processing operations in the PIMS as per ISO/IEC 17065.

(b) JT013033 (prEN 17799), a standard on "Personal data Protection requirements for processing operations" focusing on providing a basis for certifying processes and services. It specifies baseline requirements for demonstrating processing activities compliance with the European personal data protection normative framework in accordance with EN ISO/IEC 17065. Its objective is to provide a set of requirements enabling organizations to conform effectively with the European personal data protection normative framework.

Chapter 6-Legal maximum and corporate liability

Determining the undertaking's turnover and corporate liability (section 6.2, p.34)

It is our opinion that the parent company may only be considered to exercise decisive influence over the infringer company (for the purpose of including the parent company in the undertaking) where the parent company decisively influences the economic activities of the infringer in a way that decisively influences the determination, by the infringer, of the means and purpose of the processing at hand.

Yours Sincerely,

Maria Raphael

Co-ordinator of the CEN/CLC/JTC13/WG5 Consultation Task Force

ABOUT CEN AND CENELEC

CEN (European Commitee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization) are recognised by the European Union (EU) and the European Free Trade Association (EFTA) as European Standardization Organizations responsible for developing standards at European level, as per European Regulation 1025/2012. The members are the National Standards Bodies (CEN) and National Electrotechnical Committees (CENELEC) from 34 European countries. European Standards (ENs) and other standardization deliverables are adopted by CEN and CENELEC, are accepted and recognized in all of these countries. These standards contribute to enhancing safety, improving quality, facilitating cross-border trade and strengthening of the European Single Market. They are developed through a process of colaboration among experts nominated by business and industry, research institutions, consumer and environemental organizations, trade unions and other societal stakeholders. CEN and CENELEC work to promote the international alignment of standards in the framework of technical cooperation agreements with ISO (International Organization for Standardization) and the IEC (International Electrotechnical Comission).