ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 253

Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679

Adopted on 3 October 2017

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE

PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

Table of contents:

I. Introduction

The EU has completed a comprehensive reform of data protection regulation in Europe. The reform rests on several pillars (key components): coherent rules, simplified procedures, coordinated actions, user involvement, more effective information and stronger enforcement powers.

Data controllers and data processors have increased responsibilities to ensure that personal data of the individuals is protected effectively. Supervisory authorities have powers to ensure that the principles of the General Data Protection Regulation (hereafter 'the Regulation') as well as the rights of the individuals concerned are upheld according to the wording and the spirit of the Regulation.

Consistent enforcement of the data protection rules is central to a harmonized data protection regime. Administrative fines are a central element in the new enforcement regime introduced by the Regulation, being a powerful part of the enforcement toolbox of the supervisory authorities together with the other measures provided by article 58.

This document is intended for use by the supervisory authorities to ensure better application and enforcement of the Regulation and expresses their common understanding of the provisions of article 83 of the Regulation as well as its interplay with articles 58 and 70 and their corresponding recitals.

In particular, according to article 70, (1) (e), the European Data Protection Board (hereafter 'EDPB') is empowered to issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation and article 70, (1), (k) specifies the provision for guidelines concerning the setting of administrative fines.

These guidelines are not exhaustive, neither will they provide explanations about the differences between administrative, civil or criminal law systems when imposing administrative sanctions in general.

In order to achieve a consistent approach to the imposition of the administrative fines, which adequately reflects all of the principles in these guidelines, the EDPB has agreed on a common understanding of the assessment criteria in article 83 (2) of the Regulation and therefore the EDPB and individual supervisory authorities agree on using this Guideline as a common approach.

II. Principles

Once an infringement of the Regulation has been established based on the assessment of the facts of the case, the competent supervisory authority must identify the most appropriate corrective measure(s) in order to address the infringement. The provisions of article 58 (2) b-j[1] indicate which tools the supervisory authorities may employ in order to address non-compliance from a controller or a processor. When using these powers, the supervisory authorities must observe the following principles:

1. Infringement of the Regulation should lead to the imposition of "equivalent sanctions".

The concept of "equivalence" is central in determining the extent of the obligations of the supervisory authorities to ensure consistency in their use of corrective powers according to article 58 (2) in general, and the application of administrative fines in particular[2].

*In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union**, the level of protection should be equivalent** in all Member States* (recital 10). Recital 11 elaborates the fact that an equivalent level of protection of personal data throughout the Union requires, amongst others, "*equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States*.". Further more, equivalent sanctions in all Member States as well as effective cooperation between supervisory authorities of different Member States is seen as a way "*to prevent divergences hampering the free movement of personal data within the internal market*", in line with recital 13 of the Regulation.

The Regulation sets a stronger basis than Directive 95/46/EC for a greater level of consistency as the Regulation is directly applicable in the Member States. While supervisory authorities operate with "complete independence" (article 52) with respect to national governments, controllers or processors, they are required to cooperate "*with a view to ensuring the consistency of application and enforcement of this Regulation*" (article 57, (1),(g)).

The Regulation calls for a greater consistency than the Directive 95/46 when imposing sanctions. In cross border cases, consistency shall be achieved primarily through the cooperation (one –stop-shop) mechanism and to some extent through the consistency mechanism set forth by the new Regulation.

In national cases covered by the Regulation, the supervisory authorities will apply these guidelines in the spirit of cooperation according to article 57, 1 (g) and article 63, with a view to ensuring the consistency of application and enforcement of the Regulation. Although supervisory authorities remain independent in their choice of the corrective measures presented in Article 58 (2), it should be avoided that different corrective measures are chosen by the supervisory authorities in similar cases.

The same principle applies when such corrective measures are imposed in the form of fines.

[1] Article 58 (2) a provides that warnings may be issued when "processing operations are likely to infringe provisions of the Regulation". In other words, in the case covered by the provision the infringement of the Regulation has not occurred yet.

[2] Even where the legal systems in some EU countries do not allow for the imposition of administrative fines as set out in the Regulation, such an application of the rules in those Member States needs to have an equivalent effect to administrative fines imposed by supervisory authorities (recital 151). The Courts are bound by the Regulation but they are not bound by these guidelines of the EDPB.

2. Like all corrective measures chosen by the supervisory authorities, administrative fines should be "effective, proportionate and dissuasive".

Like all corrective measures in general, administrative fines should adequately respond to the nature, gravity and consequences of the breach, and supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified. The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish unlawful behavior (or both).

Supervisory authorities should identify a corrective measure that is "*effective, proportionate and dissuasive*" (art. 83 (1)), both in national cases (article 55) and in cases involving cross- border processing of personal data (as defined in article 4 (23)).

These guidelines recognize that national legislation may set additional requirements on the enforcement procedure to be followed by the supervisory authorities. This may for example include address notifications, form, deadlines for making representations, appeal, enforcement, payment[3].

Such requirements should however not hinder in practice the achievement of effectiveness, proportionality or dissuasiveness.

A more precise determination of effectiveness, proportionality or dissuasiveness will be generated by emerging practice within supervisory authorities (on data protection, as well as lessons learned from other regulatory sectors) as well as case-law when interpreting these principles.

In order to impose fines that are effective, proportionate and dissuasive, the supervisory authority shall use for the definition of the notion of an undertaking as provided for by the CJEU for the purposes of the application of Article 101 and 102 TFEU, namely that the concept of an undertaking **is understood to mean** an economic unit, which may be formed by the parent company and all involved subsidiaries. In accordance with EU law and case-law[4], an undertaking must be understood to be the economic unit, which engages in commercial/economic activities, regardless of the legal person involved (Recital 150).

3. The competent supervisory authority will make an assessment "in each individual case".

Administrative fines may be imposed in response to a wide range of infringements. Article 83 of the Regulation provides a harmonized approach to breaches of obligations expressly listed in paras (4)-(6). Member State law may extend the application of article 83 to public authorities and bodies established

[3] As an example, the constitutional framework and draft data protection legislation of Ireland, provides that a formal decision is reached on the fact of the infringement itself, which is communicated to the relevant parties, before an assessment of the scale of the sanction(s). The decision on the fact of the infringement itself cannot be revisited during the assessment of the scale of the sanction(s).

[4] The ECJ case law definition is: «the concept of an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed" (Case Höfner and Elsner, para 21, ECLI:EU:C:1991:161). An undertaking «must be understood as designating an economic unit even if in law that economic unit consists of several persons, natural or legal» (Case Confederación Española de Empresarios de Estaciones de Servicio [para 40, ECLI:EU:C:2006:784).

in that Member State. Additionally, Member State law may allow for or even mandate the imposition of a fine for infringement of other provisions than those mentioned in article 83 (4)-(6).

The Regulation requires assessment of each case individually[5]. Article 83 (2) is the starting point for such an individual assessment. The paragraph states "*when deciding whether to impose an administrative fine, and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following…*"Accordingly, and also in the light of Recital 148[6] the supervisory authority has the responsibility of choosing the most appropriate measure(s). In the cases mentioned in Article 83 (4) – (6), this choice **must** include consideration of all of the corrective measures, which would include consideration of the imposition of the appropriate administrative fine, either accompanying a corrective measure under Article 58(2) or on its own.

Fines are an important tool that supervisory authorities should use in appropriate circumstances. The supervisory authorities are encouraged to use a considered and balanced approach in their use of corrective measures, in order to achieve both an effective and dissuasive as well as a proportionate reaction to the breach. The point is to not qualify the fines as last resort, nor to shy away from issuing fines, but on the other hand not to use them in such a way which would devalue their effectiveness as a tool.

The EDPB, when competent according to article 65 of the Regulation, will issue a binding decision on disputes between authorities relating in particular to the determination of the existence of an infringement. When the relevant and reasoned objection raises the issue of the compliance of the corrective measure with the GDPR, the decision of EDPB will also discuss how the principles of effectiveness, proportionality and deterrence are observed in the administrative fine proposed in the draft decision of the competent supervisory authority . EDPB guidance on the application of article 65 of the Regulation will follow separately for further detail on the type of decision to be taken by the EDPB.

[5] Further to the application of article 83 criteria there are other provisions to bolster the foundation of this approach such as:

- recital 141 "*the investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case*."
- recital 129 "*The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…".*
- article 57(1) (f) "*handle complaints lodged by a data subject, or by a body, organisation or association in accordance with article 8, and investigate to the extent appropriate, the subject matter of the complaint*."

[6] "*In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process*".

4. A harmonized approach to administrative fines in the field of data protection requires active participation and information exchange among Supervisory Authorities

These guidelines acknowledge that fining powers represent for some national supervisory authorities a novelty in the field of data protection, raising numerous issues in terms of resources, organization and procedure. Notably, the decisions in which the supervisory authorities exercise the fining powers conferred to them will be subject to appeal before national courts.

Supervisory authorities shall cooperate with each other and where relevant, with the European Commission through the cooperation mechanisms as set out in the Regulation in order to support formal and informal information exchanges, such as through regular workshops. This cooperation would focus on their experience and practice in the application of the fining powers to ultimately achieve greater consistency.

This proactive information sharing, in addition to emerging case law on the use of these powers, may lead to the principles or the particular details of these guidelines being revisited.

III. Assessment criteria in article 83 (2)

Article 83 (2) provides a list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine. This does not recommend a repeated assessment of the same criteria, but an assessment that takes into account all the circumstances of each individual case, as provided by article 83[7].

The conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of the fine, thereby avoiding the need to assess using the same criteria twice.

This section provides guidance for the supervisory authorities of how to interpret the individual facts of the case in the light of the criteria in article 83 (2).

(a) the nature, gravity and duration of the infringement

Almost all of the obligations of the controllers and processors according to the Regulation are categorised according to their **nature** in the provisions of article 83(4) – (6) . The Regulation, in setting up two different maximum amounts of administrative fine (10/20 million Euros), already indicates that a breach of some provisions of the Regulation may be more serious than for other provisions. However the competent supervisory authority, by assessing the facts of the case in light of the general criteria provided in article 83 (2), may decide that in the particular case there is a higher or a more reduced need to react with a corrective measure in the form of a fine. Where a fine has been chosen as the one or one of several appropriate corrective measure(s), the tiering system of the Regulation (article 83 (4)- 83 (6)) will be applied in order to identify the maximum fine that can be imposed according to the nature of the infringement in question.

Recital 148 introduces the notion of "minor infringements". Such infringements may constitute breaches of one or several of the Regulation's provisions listed in article 83 (4) or (5). The assessment of the criteria in article 83 (2) may however lead the supervisory authority to believe that in the concrete circumstances of the case, the breach for example, does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation in question. In such cases, the fine may (but not always) be replaced by a reprimand.

Recital 148 does not contain an obligation for the supervisory authority to always replace a fine by a reprimand in the case of a minor infringement ("*a reprimand may be issued instead of a fine*"), but rather a possibility that is at hand, following a concrete assessment of all the circumstances of the case.

Recital 148 opens up the same possibility to replace a fine by a reprimand , where the data controller is a natural person and the fine likely to be imposed would constitute a disproportionate burden. The starting point is that the supervisory authority has to assess whether, considering the circumstances of the case at hand, the imposition of a fine is required. If it finds in favour of imposing a fine, then the supervisory authority must also assess whether the fine to be imposed would constitute a disproportionate burden to a natural person.

Specific infringements are not given a specific price tag in the Regulation, only a cap (maximum amount). This can be indicative of a relative lower degree of gravity for a breach of obligations listed in article 83(4), compared with those set out in article 83(5). The effective, proportionate and dissuasive reaction to a breach of article 83(5) will however depend on the circumstances of the case.

[7] The assessment of the sanction to be applied may come separately after the assessment of whether there has been an infringement due to national procedural rules arising from constitutional requirements in some countries. Therefore, this may limit the content and the amount of detail in a draft decision issued by lead supervisory authority in such countries.

It should be noticed that breaches of the Regulation, which by their nature might fall into the category of "up to 10 million Euros or up to 2% of total annual worldwide turnover" as set out in article 83 (4), might end up qualifying for a higher tier (Euro 20 million) category in certain circumstances. This would be likely to be the case where such breaches have previously been addressed in an order from the supervisory authority, an order[8] which the controller or processor failed to comply with[9] (article 83 (6)). The provisions of the national law may in practice have an impact on this assessment[10]. The nature of the infringement, but also "*the scope, purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them*", will be indicative of the **gravity** of the infringement. The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement. Therefore, if an infringement of article 8 and article 12 has been discovered, then the supervisory authority may be able to apply the corrective measures as set out in article 83(5) which correspond to the category of the gravest infringement, namely article 12. More detail at this stage is beyond the scope of this particular guideline (as detailed calculation work would be the focus of a potential subsequent stage of this guideline).

The factors below should be assessed in combination eg. the number of data subjects together with the possible impact on them.

The number of data subjects involved should be assessed, in order to identify whether this is an isolated event or symptomatic of a more systemic breach or lack of adequate routines in place. This is not to say that isolated events should not be enforceable, as an isolated event could still affect a lot of data subjects. This will, depending on the circumstances of the case, be relative to, for example, the total number of registrants in the database in question, the number of users of a service, the number of customers, or in relation to the population of the country, as appropriate.

[8] The orders, provided in article 58 (2) are:

- to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
- to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- to order the controller to communicate a personal data breach to the data subject;
- to impose a temporary or definitive limitation including a ban on processing
- to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- to order the suspension of data flows to a recipient in a third country or to an international organisation.

[9] Application of article 83(6) necessarily must take into account national law on procedure. National law determines how an order is issued, how it is notified, from which point it takes effect, whether there is a grace period to work on compliance. Notably, the effect of an appeal on the enforceability of an order should be taken into account.

[10] Statutory provisions of limitation may have the effect that a previous order of the supervisory authority may no longer be taken in to consideration due to the amount of time that has lapsed since that previous order was issued. In some jurisdictions, rules require that after the prescription period has passed with respect to an order, no fine may be imposed for non-compliance with that order under article 83(6). It will be up to each supervisory authority in each jurisdiction to determine how such impacts will affect them.

The purpose of the processing must also be assessed. The WP 29 opinion on "purpose limitation"[11] previously analysed the two main building blocks of this principle in data protection law: purpose specification and compatible use. When assessing the purpose of the processing in the context of article 83 (2), the supervisory authorities should look into the extent to which the processing upholds the two key components of this principle[12]. In certain situations, the supervisory authority might find it necessary to factor in a deeper analysis of the purpose of the processing in itself in the analysis of article 83 (2).

If the data subjects have suffered **damage**, the level of the damage has to be taken into consideration. Processing of personal data may generate risks for the rights and freedoms of the individual, as illustrated by recital 75:

> "*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects*."

If damages have been or are likely to be suffered due to the infringement of the Regulation then the supervisory authority should take this into account in its choice of corrective measure, although the supervisory authority itself is not competent to award the specific compensation for the damage suffered.

The imposition of a fine is not dependent on the ability of the supervisory authority to establish a causal link between the breach and the material loss (see for example article 83 (6)).

Duration of the infringement may be illustrative of, for example:

a) wilful conduct on the data controller's part, or

b) failure to take appropriate preventive measures, or

c) inability to put in place the required technical and organisational measures.

(b) the intentional or negligent character of the infringement

In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.

---

[11] WP 203 , Opinion 03/2013 on purpose limitation, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] See also Wp 217, opinion 6/2014 on the notion of legitimate interest of the data controller under article 7, page 24, on the question: "What makes an interest "legitimate" or "illegitimate"?"

It is generally admitted that intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine. The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case. In addition, emergent case law and practice in the field of data protection under the application of the Regulation will be illustrative of circumstances indicating clearer thresholds for assessing whether a breach was intentional.

Circumstances indicative of intentional breaches might be unlawful processing authorised explicitly by the top management hierarchy of the controller, or in spite of advice from the data protection officer or in disregard for existing policies, for example obtaining and processing data about employees at a competitor with an intention to discredit that competitor in the market.

Other examples here might be:

- amending personal data to give a misleading (positive) impression about whether targets have been met – we have seen this in the context of targets for hospital waiting times
- the trade of personal data for marketing purpose ie selling data as 'opted in' without checking/disregarding data subjects' views about how their data should be used

Other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them)may be indicative of negligence.

Enterprises should be responsible for adopting structures and resources adequate to the nature and complexity of their business. As such, controllers and processors cannot legitimise breaches of data protection law by claiming a shortage of resources. Routines and documentation of processing activities follow a risk-based approach according to the Regulation.

There are grey areas which will affect decision-making in relation to whether or not to impose a corrective measure and the authority may need to do more extensive investigation to ascertain the facts of the case and to ensure that all specific circumstances of each individual case were sufficiently taken into account.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

The data controllers and processors have an obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, to carry out data protection impact assessments and mitigate risks arising form the processing of personal data to the rights and freedoms of the individuals. However, when a breach occurs and the data subject has suffered damage, the responsible party should do whatever they can do in order to reduce the consequences of the breach for the individual(s) concerned. Such responsible behaviour (or the lack of it) would be taken into account by the supervisory authority in their choice of corrective measure(s) as well as in the calculation of the sanction to be imposed in the specific case.

Although aggravating and mitigating factors are particularly suited to fine-tune the amount of a fine to the particular circumstances of the case, their role in the choice of appropriate corrective measure should not be underestimated. In cases where the assessment based on other criteria leaves the supervisory authority in doubt about the appropriateness of an administrative fine, as a standalone corrective measure, or in combination with other measures in article 58, such aggravating or attenuating circumstances may help to choose the appropriate measures by tipping the balance in favour of what proves more effective, proportionate and dissuasive in the given case.

This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a

reckless/ negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.

Regulatory experience from SAs under the 95/46/EC Directive has previously shown that it can be appropriate to show some degree of flexibility to those data controllers/processors who have admitted to their infringement and taken responsibility to correct or limit the impact of their actions. This might include examples such as (although this would not lead to a more flexible approach in every case):

- contacting other controllers/processors who may have been involved in an extension of the processing e.g. if there has been a piece of data mistakenly shared with third parties.
- timely action taken by the data controller/processor to stop the infringement from continuing or expanding to a level or phase which would have had a far more serious impact than it did.

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

The Regulation has introduced a far greater level of accountability of the data controller in comparison with the EC Data Protection Directive 95/46/EC.

The degree of responsibility of the controller or processor assessed against the backdrop of applying an appropriate corrective measure may include:

- Has the controller implemented technical measures that follow the principles of data protection by design or by default (article 25)?
- Has the controller implemented organisational measures that give effect to the principles of data protection by design and by default (article 25) at all levels of the organisation?
- Has the controller/processor implemented an appropriate level of security (article 32)?
- Are the relevant data protection routines/policies known and applied at the appropriate level of management in the organisation? (Article 24).

Article 25 and article 32 of the Regulation require that the controllers "*take into account the state of the art, the cost of implementation and the nature, scope, context, and purposes of the processing, as well as the risks of varying likelihood and severity for rights and freedoms for the natural persons posed by the processing*". Rather than being an obligation of goal, these provisions introduce obligations of means, that is, the controller must make the necessary assessments and reach the appropriate conclusions. The question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.

In this assessment, due account should be taken of any "best practice" procedures or methods where these exist and apply. Industry standards, as well as codes of conduct in the respective field or profession are important to take into account. Codes of practice might give an indication as to what is common practice in the field and an indication of the level of knowledge about different means to address typical security issues associated with the processing.

While best practice should be the ideal to pursue in general, the special circumstances of each individual casemust be taken into account when making the assessment of the degree of responsibility.

(e) any relevant previous infringements by the controller or processor;

This criterion is meant to assess the track record of the entity committing the infringement. Supervisory authorities should consider that the scope of the assessment here can be quite wide because any type of breach of the Regulation, though different in nature to the one being investigated now by the supervisory authority might be "relevant" for the assessment, as it could be indicative of a general level of insufficient knowledge or disregard for the data protection rules.

The supervisory authority should assess:

- Has the controller/processor committed the same infringement earlier?
- Has the controller/ processor committed an infringement of the Regulation in the same manner? (for example as a consequence of insufficient knowledge of existing routines in the organisation, or as a consequence of inappropriate risk assessment, not being responsive to requests from the data subject in a timely manner, unjustified delay in responding to requests and so on).

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

Article 83 (2) provides that the degree of cooperation may be given "due regard" when deciding whether to impose an administrative fine and in deciding on the amount of the fine. The Regulation does not give a precise answer to the question how to take into account the efforts of the controllers or the processors to remedy an infringement already established by the supervisory authority. Moreover, it is clear that the criteria would usually be applied when calculating the amount of the fine to be imposed.

However, where intervention of the controller has had the effect that negative consequences on the rights of the individuals did not produce or had a more limited impact than they could have otherwise done, this could also be taken into account in the choice of corrective measure that is proportionate in the individual case.

One example of a case where cooperation with the supervisory authority might be relevant to consider might be:

- Has the entity responded in a particular manner to the supervisory authority's requests during the investigation phase in that specific case which has significantly limited the impact on individuals' rights as a result?

This said, it would not be appropriate to give additional regard to cooperation that is already required by law for example, the entity is in any case required to allow the supervisory authority access to premises for audits/inspections.

(g) the categories of the personal data affected by the infringement;

Some examples of key questions that the supervisory authority may find it necessary to answer here, if appropriate to the case, are:

- Does the infringement concern processing of special categories of data set out in articles 9 or 10 of the Regulation?
- Is the data directly identifiable/ indirectly identifiable?
- Does the processing involve data whose dissemination would cause immediate damage/distress to the individual (which falls outside the category of article 9 or 10)?

- Is the data directly available without technical protections, or is it encrypted[13]?

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

A supervisory authority might become aware about the infringement as a result of investigation, complaints, articles in the press, anonymous tips or notification by the data controller. The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement.

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

A controller or processor may already be on the supervisory authority's radar for monitoring their compliance after a previous infringement and contacts with the DPO where they exist are likely to have been extensive. Therefore, the supervisory authority will take into account the previous contacts.

As opposed to the criteria in (e), this assessment criteria only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors "*with regard to the same subject matter"*.

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;

Supervisory authorities have a duty to "*monitor and enforce the application of this Regulation*, (article 57 1 (a))". Adherence to approved codes of conduct may be used by the controller or processor as an way to demonstrate compliance, according to articles 24 (3), 28 (5) or 32 (3).

In case of a breach of one of the provisions of the Regulation, adherence to an approved code of conduct might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure from the supervisory authority. Approved codes of conduct will, according to article 40 (4) contain "*mechanisms which enable the (monitoring) body to carry out mandatory monitoring of compliance with its provisions*".

Where the controller or processor has adhered to an approved code of conduct, the supervisory authority may be satisfied that the code community in charge of administering the code takes the appropriate action themselves against their member, for example through the monitoring and enforcement schemes of the code of conduct itself. Therefore, the supervisory authority might consider that such measures are effective, proportionate or dissuasive enough in that particular case without the need for imposing additional measures from the supervisory authority itself. Certain forms of sanctioning non-compliant behaviour may be made through the monitoring scheme, according to article 41 (2) c and 42 (4), including suspension or exclusion of the controller or processor concerned from the code community. Nevertheless, the powers of the monitoring body are "*without prejudice to the tasks and powers of the competent supervisory authority*", which means that the supervisory authority is not under an obligation to take into account previously imposed sanctions pertaining to the self-regulatory scheme.

[13] It shouldn't always be considered 'a bonus' mitigating factor that the breach only concerns indirectly identifiable or even pseudonymous/encrypted data. For those breaches, an overall assessment of the other criteria might give a moderate or strong indication that a fine should be imposed.

Non-compliance with self-regulatory measures could also reveal the controller's/processor's negligence or intentional behaviour of non-compliance.

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

The provision itself gives examples of which other elements might be taken into account when deciding the appropriateness of an administrative fine for an infringement of the provisions mentioned in Article 83(4-6).

Information about profit obtained as a result of a breach may be particularly important for the supervisory authorities as economic gain from the infringement cannot be compensated through measures that do not have a pecuniary component. As such, the fact that the controller had profited from the infringement of the Regulation may constitute a strong indication that a fine should be imposed.

IV.Conclusion

Reflections on the questions such as those provided in the previous section will help supervisory authorities identify, from the relevant facts of the case, those criteria which are most useful in reaching a decision on whether to impose an appropriate administrative fine in addition to or instead of other measures under Article 58. Taking into account the context provided by such assessment, the supervisory authority will identify the most effective, proportionate and dissuasive corrective measure to respond to the breach.

Article 58 provides some guidance as to which measures a supervisory authority might choose, as the corrective measures in themselves are different in nature and suited primarily for achieving different purposes. Some of the measures in article 58 may even be possible to cumulate, therefore achieving a regulatory action comprising more than one corrective measure.

It is not always necessary to supplement the measure through the use of another corrective measure. For example: The effectiveness and dissuasiveness of the intervention by the supervisory authority with its due consideration of what is proportionate to that specific case may be achieved through the fine alone.

In essence, authorities need to restore compliance through all of the corrective measures available to them. Supervisory authorities will also be required to choose the most appropriate channel for pursuing regulatory action. For example, this could include penal sanctions (where these are available at national level).

The practice of applying administrative fines consistently across the European Union is an evolving art. Actions should be taken by supervisory authorities working together to improve consistency on an ongoing basis. This can be achieved through regular exchanges through case-handling workshops or other events which allow the comparison of cases from the sub-national, national and cross-border levels. The creation of a permanent sub-group attached to a relevant part of the EDPB is recommended to support this ongoing activity.