GUIDELINES FOR THE CALCULATION OF ADMINISTRATIVE FINES UNDER THE GDPR

On 14 March 2019, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* – **'AP'**) published new Guidelines on Administrative Fines 2019 (*Boetebeleidsregels Autoriteit Persoongegevens 2019* – **'Guidelines**'). It is a sign on the wall that the Dutch regulator is preparing itself for a new phase in its enforcement of the new data protection regime set by the General Data Protection Regulation (GDPR) and the Dutch GDPR Implementation Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming* – **'UAVG'**). The publication of the Guidelines sends a clear message to organisations: fines are coming!

BACKGROUND

It is undeniable that part of the GDPR's fame and impact are due to its significant administrative fines for both data controllers and data processors. Violations of the provisions listed in Article 83(5)[1] GDPR can be punished with a maximum fine of to 20 million euros or 4% of the total global turnover of the preceding fiscal year, whichever is higher. For other GDPR violations which are generally considered to be less serious, regulators may 'only' impose a fine up to 10 million euros or 2% of the global turnover. These momentous fines are often emphasized by EU regulators and data protection officers alike to promote and stimulate GDPR compliance.

When the fines and the enforcement regime are looked at in more detail however, it is not self-evident that such high fines will follow from just any violation of the GDPR. The leading principle from a European perspective is that administrative fines must be effective, proportionate and dissuasive.[2] When deciding whether to impose an administrative fine and deciding on the amount of the fine, regulators must always consider the circumstances of each individual case.

In particular, they must take into account the factors mentioned in article 83(2) GDPR such as nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, any action taken to mitigate damage, the degree of responsibility of the controller or processor, any relevant previous infringements, the degree of cooperation with the regulator and other aggravating or mitigating factors. This aims to ensure that fines are properly tailored to the circumstances of the case at hand. Considering this, there would only be room to impose the maximum penalty under exceptional circumstances.

Each EU regulator must consider a substantial number of non-exhaustive criteria when administering a fine, and all within the local legal system of administrative laws and traditions. It will come as no surprise that this leaves room for diverging practices and varying fines for comparable cases. In order to achieve a consistent approach for the application of the administrative fines, the European Data Protection Board (**'EDPB'**) has published *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679* ("**EDPB Guidelines**") in January 2018. While these EDPB

[1] Art. 83(5) GDPR refers to the basic principles for processing pursuant to art. 5, 6, 7 and 9; the data subjects' rights pursuant to art 12 - 22; transfers of personal data pursuant to art 44 - 49; any national obligations as adopted under Chapter IX; non-compliance with an order or a limitation on processing or the suspension of data flows by the DPA pursuant to art. 58(2) or failure to provide access in violation of art 58(1) GDPR.

[2] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, p. 17.

Guidelines shed more light on when to impose a fine and how to interpret the factors of Article 83(2), they do not contain guidance on how to set and calculate a fine for a particular case.

While the EDPB intends to issue further guidelines to ensure consistency in applying and calculating administrative fines across the EU, it is not clear when these guidelines can be expected. Against this background, the Dutch DPA has now taken the opportunity to adopt national Guidelines until further EDPB Guidelines are provided. While adopting these Guidelines is as such not required to impose a fine under Dutch administrative law, regulators frequently adopt such guidelines to provide more legal certainty and to avoid difficult discussions in court.

Should the EDPB decide to publish EPDB Guidelines for the calculation of fines under GDPR, the Dutch DPA will in principle withdraw its Guidelines accordingly. From that perspective, the new Guidelines only have a temporary status. However, it is not impossible that the EDPB might draw some inspiration from the Dutch Guidelines too. A good reason to look at these Guidelines in more detail.

OVERVIEW OF THE NEW GUIDELINES

The new Guidelines replace the Guidelines Administrative Fines issued by the AP in 2016, which were based on the old Dutch Data Protection Act, the *Wet bescherming persoonsgegevens* ('**Wbp**'). In essence, the new guidelines continue and build on the 2016 guidelines, taking the GDPR into account.

The Guidelines contain concrete rules for the calculation of fines for violation of the GDPR and the UAVG, as well as for violations of other laws for which the AP is the supervisory authority and has the power to impose a fine. This includes for example a telecom-specific data breach notification obligation in Article 11.3a of the Dutch Telecommunications Act.

In the Guidelines the AP has grouped infringements by legal penalty maximum and divided them into three categories with increasing administrative fines based on the seriousness of the violation. An exception is made for infringements of the GDPR for which the AP can impose an administrative fine up to EUR 20,000,000 or 4% of the total worldwide annual turnover. These infringements are divided into four categories, not three. Annex 2 describes which provisions of the GPDR and the UAVG fall in which category.

Each category is linked to a specific bandwidth that the AP considers to be "appropriate and required". This means that the fining bandwidth is considered by the AP to be proportional on the one hand and sufficiently dissuasive for both the offender (special prevention) and other potential offenders (general prevention) on the other. Within the chosen bandwidth the AP has determined a standard penalty which will be the "starting point" for the calculation of the fine. For violations of the GDPR these are as follows:

Category	**Standard fine bandwidth**	**Standard penalty**
I	EUR 0 – 200.000	EUR 100.000
II	EUR 120.000 – 500.000	EUR 310.000
III	EUR 300.000 – 750.000	EUR 525.000
IV*	EUR 450.000 – 1.000.000	EUR 725.000
* Only in case the legal maximum penalty of EUR 20.000.000/ 4% turnover applies.		

After determining the standard penalty, the fine is further calculated by looking at the factors in Article 7 of the Guidelines. These factors are directly derived from Article 83(2) GDPR and can be seen as indicators of the seriousness of the violation and the degree of responsibility of the offender. These factors will be used as pluses or minuses on the standard penalty when calculating the fine. The AP will normally stay within the designated bandwidth, but if the circumstances of the case give cause to do so, the AP may 'push forward or push back' in the penalty bandwidth of the next higher or next lower category.

In case of a repeat offence the fine will automatically be increased with 50%, unless this would be disproportionate in the circumstances of the case. Under the Guidelines there is a repeat offence "when at the time the offence was committed there were not yet five years passed since the imposition of an administrative fine by the AP on the offender in respect of the same or a similar offence committed by the offender". Given this definition, other measures such as warnings, reprimands or orders under penalties will not trigger a qualification as repeat offence. Parties which have been found guilty by the AP of a violation of data protection rules in the past, but were not fined, will likely be happy to hear that.

The Guidelines still leave the AP a certain room for the imposition of the very high penalty maximums mentioned in the GDPR (see in particular Article 8.3 and 8.4 of the Guidelines), but this likely only becomes relevant in exceptional cases. Normally, the AP will calculate the fine by applying the method in the Guidelines. The resulting fines may not be as high as some were afraid of, but of course they can still be quite substantial.

This is in particular true in case of multiple violations caused by the same or linked processing activities. According to Article 10 of the Guidelines, the AP may then impose multiple fines up to the legal maximum of the most severe violation. Here, the Guidelines seem to leave the AP considerable freedom to determine the fine – with the constraint that the total amount of the fine always has to be proportionate considering the circumstances of the case.

NOTEWORTHY POINTS

One thing that really stands out when looking at the Guidelines is that the bandwidths and standard penalties are far lower than the maximum penalties of the GDPR and are pretty much in line with the penalty amounts in other areas of Dutch law. The highest bandwidth mentioned in the Guidelines is 'only' EUR 1 million and the highest standard penalty EUR 725.000 for violations of the rules regarding processing of special categories of personal data and automated individual decision making. This method seems to indicate that the high penalty maximums of the GDPR will normally not come into play.

Also remarkable is that the Guidelines do not seem to leave room for turnover based fines in normal cases. The designated bandwidth and the standard penalty are namely not connected in any way to the turnover of an organisation. Perhaps the AP believes this would be too difficult, as the GDPR does not say how the turnover should be determined. It is a fact that it can be quite challenging to determine the relevant turnover linked to the violation. This does not mean that the AP will never impose turnover based fines, but it can only do so if it goes outside of the Guidelines, i.e. in exceptional cases when the application of the Guidelines would not lead to an effective, proportionate and dissuasive fine.

IMPACT OF THE GUIDELINES

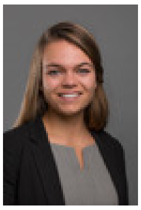
In January 2019, the French regulator was the first DPA to impose a very high and turnover based fine since the GDPR entered into force. It imposed a financial fine of 50 million euros on Google for violating the transparency and consent requirements with regard to its data processing activities for personalized advertising purposes.

As this would likely qualify as an exceptional case which could justify a deviation from the Guidelines, it is not unthinkable that the AP would have imposed a similar fine in such a situation. However, given the Guidelines it is clear that in most cases fines of that magnitude are unlikely to be imposed by the AP.

It could come as a relief for some companies that the Guidelines avoid the GDPR's maximum penalties and provide a bit more nuance when it comes to the calculation of fines. Companies should however take the Guidelines as a clear signal from the AP to the market that it will not shy away from imposing substantial fines. The AP has already announced that the first GDPR fines will be coming in 2019. With the Guidelines the AP has now implemented a proper framework for the calculation of the fines, taking into account its new powers under the GDPR.

Although these Guidelines are primarily written for the AP itself, it is quite possible that the Guidelines will have a wider impact. As the Dutch regulator is the first data protection authority to issue guidelines for the calculation of fines for a piece of EU legislation, other regulators may follow the approach set out by the AP when calculating fines. To this extent, the new Guidelines on Administrative Fines might turn out to be relevant for a wider audience across the EU.

If you want to know more about the new Guidelines or have other questions with regard to data protection, please feel free to reach out to one of our experts below.

 Wilfred Steenbruggen	 Sonja van Harten	 Berend van der Eijk