GIBSON DUNN

October 30, 2019

GDPR: FINING GUIDELINES WILL INCREASE EXPOSURE IN GERMANY

To Our Clients and Friends:

In October 2019, the German Conference of Federal and State Data Protection Authorities (the "**DSK**") published its long-awaited guidelines for the determination of fines in privacy violation proceedings against companies (the "**Fining Concept**").[1]

The Fining Concept applies to the imposition of fines by German Data Protection Authorities within the scope of the European General Data Protection Regulation ("**GDPR**"). According to the DSK, the Fining Concept is intended to provide for a uniform, comprehensible, transparent and case-by-case method of determining fines. The central starting point for the determination of the fine is the global annual turnover of a company in the preceding business year.

As a consequence, in the future, we will likely be seeing significantly higher GDPR fines in Germany more in the range of the higher end of the maximum fine limits laid out in Article 83 GDPR – up to 4 % of a company's global annual group-wide turnover. The application of corporate liability principles, which were originally developed under EU antitrust law, may also heighten the stakes. Noteworthy, the Fining Concept has been tested in actual cases already,[2] leading to an increase in fines.

It is important, though, that the Fining Concept is neither binding on data protection authorities outside Germany, nor for cross-border cases, nor for the review of fines by the German national courts.

METHODOLOGY OF THE FINING CONCEPT

The methodology introduced by the DSK is complex and involves five steps:

STEPS 1 and 2: The company concerned is classified into a size category depending on its turnover (micro, small and medium-sized enterprises and large enterprises) – each with various subgroups, which are meant to provide for a more precise individual turnover range. The average annual turnover of the relevant subgroup is then determined. For corporations achieving an annual turnover of more than EUR 500 million, the actual turnover will be considered.

STEP 3: A so-called "economic base value" is determined by dividing the annual average turnover amount of the relevant subgroup by 360 days and thus calculating an average "daily fining amount". On average, this daily fining amount corresponds to almost 0.28 % of a company's global annual group-wide turnover.

STEP 4: The daily fining amount will be multiplied by a factor dependent on the seriousness of the violation, which is to be assessed by the Data Protection Authority on the basis of concrete, fact-related circumstances of the individual case. The seriousness of the violation ranges from "minor", "medium", "severe" to "very severe".

For "minor" infringements of the GDPR, this multiplier is determined from a range between 1 and 4 (between 1 and 2 for mere formal violations of the GDPR). For "severe" infringements, the multiplier increases to a range between 8 and 12 (between 4 and 6 for mere formal violations), and can even be higher for "very severe" infringements. Formal violations of the GDPR include, inter alia, a violation of the obligations (i) to obtain valid consent for the processing of personal data of children, (ii) to maintain records of processing activities, (iii) to carry out a data protection impact assessment if so required, (iv) to designate a qualified data protection officer, and (v) to notify the competent data protection authority in case of a personal data breach in accordance with the applicable timeline. Substantive violations of the GDPR include, inter alia, a violation of (i) the general principles relating to the processing of personal data (e.g., processing of personal data without consent or other legal basis), (ii) the data controller's transparency and notification obligations and the data subject's related rights, and (iii) the obligations in connection with the transfer of personal data to third countries (such as the U.S.).

STEP 5: The value determined in Step 4 may then be adjusted on the basis of individual circumstance of the case – in particular with respect to mitigating and aggravating factors. Such factors may include, inter alia, the nature, gravity and duration of the violation, the intentional or negligent character of the infringement, any action taken by the controller or processor to mitigate the effects of the violation, the degree of cooperation with the competent data protection authority and any relevant previous infringements by the data controller or processor. Additionally, the Data Protection Authority deciding on the fine takes into account any other circumstances, such as the offender's ability to pay the fine and the duration of the proceedings.

As a matter of course, the overall fine limits in Article 83 GDPR (2 % for formal, 4 % for substantive data protection violations) cannot be exceeded.

GROUP CONCEPT AND PARENTAL LIABILITY

It is important to note that both the GDPR and the Fining Concept make reference to two key concepts from EU antitrust enforcement principles:

First, the GDPR and the Fining Concept explicitly refer to Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU) and the "undertakings" concept established therein. For companies to be fined, this means that all entities belonging to a corporate group (based on a concept of control) will be taken into account when assessing the annual turnover. Originally, this concept was introduced for the determination of fines in cartel proceedings, but now may have far reaching consequences for GDPR violations as well.

For the purposes of the Fining Concept, the application of the "undertakings" concept means that possibly the turnover of all companies linked to the offending company and exercising positive or even negative control (i.e., ability to block strategic decisions with a veto right) might be taken into account.

Second, parent entities may be held liable for GDPR violations committed by their subsidiaries, as long as the companies concerned are considered a so-called "single economic unit" because the parent has "decisive influence" over the offending company and is exercising that influence (so-called parental liability).[3] In other words, authorities may be able to pierce the corporate veil by going up the corporate chain to hold the ultimate parent (and potentially even its management) liable. Parental liability poses a risk for non-EU parent companies as well, since the GDPR has extensive extraterritorial reach. See our earlier client update on this subject.[4]

As a consequence, parent companies may be liable for the GDPR violations committed by their subsidiaries hence the fine notice from the respective German Data Protection Authority might be addressed to them.

However, there is no case law on these issues yet, and it remains to be seen whether the courts will strictly follow the "undertakings" concept rules which were originally developed for antitrust enforcement cases.

OUTLOOK

It is hard to predict how the individual German Data Protection Authorities will apply the Fining Concept in practice, especially with regard to steps 4 and 5 which contain a rather broad margin of discretion when determining the fine. However, taking into account that the Fining Concept foresees a multiplication of the "daily fining amount" by a factor of 1 to 4 even for minor infringements, we will probably see the German Data Protection Authorities following in the footsteps of the French Data Protection Authority ("**CNIL**") (*see* our recent client alert here[5]) and the British Information Commissioner's Office ("**ICO**") who recently indicated the intent to hand out fines in the double-digit millions area. This is already evident by the Berlin Data Protection Authority's recent announcement of its intention to impose a double-digit millions fine against an unnamed company.[6]

Strictly applied, the Fining Concept will mean that any violation of mere formal requirements of the GDPR would result in seven digit dollar fines if the offender's annual turnover exceeds a threshold of approximately USD 340 million (subject to a potential reduction in Step 5).

The Fining Concept has also received some criticism already. In particular, commentators allege that it violates the proportionality principle as set out in Article 83(1) GDPR. However, the concept might not be long-lived, since the European Data Protection Board ("**EDPB**"), which is composed of representatives of the national data protection authorities, is expected to adopt its own fining concept in the near future superseding the Fining Concept of the DSK.[7]

However, the race to the top will likely continue until the EDPB steps in and issues its own guidance – in particular to ensure a uniform GDPR enforcement throughout the EU, to prevent any attempts of forum shopping and to honor the GDPR's principle of proportionality.

---

[1] *See* DSK, *Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen* (14 October 2019), available at (German): https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf.

[2] *See* DSK press release, *DSK entwickelt Konzept zur Bußgeldzumessung* (17 September 2019), available at (German): https://www.datenschutzkonferenz-online.de/media/pm/20190917_bu%C3%9Fgeldkonzept.pdf.

[3] This concept was first established by the „*Akzo Nobel*" case decided by the European Court of Justice in 2009: C-97/08 – *Akzo Nobel NV*, 10 September 2009, ECLI:EU:C:2009:536, available at: http://curia.europa.eu/juris/document/document.jsf?docid=72629.

[4] *See* Gibson Dunn, *The General Data Protection Regulation: A Primer for U.S.-Based Organizations That Handle EU Personal Data* (Dec. 4, 2017), available at: https://www.gibsondunn.com/the-general-data-protection-regulation-a-primer-for-u-s-based-organizations-that-handle-eu-personal-data/.

[5] *See* Gibson Dunn, *The French Data Protection Authority Imposes a 50 Million Euros Fine on Google LLC* (24 January 2019), available at: https://www.gibsondunn.com/french-data-protection-authority-imposes-50-million-euros-fine-on-google-llc/.

[6] *See* Sueddeutsche Zeitung, *Berlin will Datenschutz-Bußgeld in Millionenhöhe verhängen* (13 August 2019), available in German at: https://www.sueddeutsche.de/politik/datenschutz-berlin-berlin-will-datenschutz-bussgeld-in-millionenhoehe-verhaengen-dpa.urn-newsml-dpa-com-20090101-190813-99-446541.

[7] For now the EDPB has endorsed the GDPR related guidelines of the former Article 29 Working Party which, however, made only very limited reference to turnover-based concepts for the determination of fines under the GDPR. *See* Article 29 Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679* (3 October 2017), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

The following Gibson Dunn lawyers prepared this client update: Michael Walther, Kai Gesing and Selina Grün.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these issues. For further information, please contact the Gibson Dunn lawyer with whom you usually work or any of the following leaders and members of the firm's Privacy, Cybersecurity and Consumer Protection practice group:

Europe

Ahmed Baladi - Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)

Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
James A. Cox - London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)

United States
Alexander H. Southwell - Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
M. Sean Royall - Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Olivia Adendorff - Dallas (+1 214-698-3159, oadendorff@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

Asia
Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)