KNOW-HOW

Gleiss Lutz

11.11.2019

DATA PROTECTION

VIOLATION OF DUTIES TO ERASE DATA – BERLIN'S DATA PROTECTION AUTHORITY IMPOSES 14.5 MILLION EURO FINE

On 30 October 2019, Berlin's Commissioner for Data Protection and Freedom of Information imposed a fine of roughly 14.5 million euros on a housing company for having violated the General Data Protection Regulation (GDPR). To date, the highest fines imposed in Germany under the GDPR had been around 195,000 euros, but the fine now imposed is the first in Germany to exceed the one million euro mark (by a large margin). It also represents the highest fine that a data protection authority has ever imposed on a company in Germany. The large sum involved in the fine also derives from the new concept for calculating fines that was recently published by Germany's Conference of the Data Protection Commissioners of the Federation and of the Laender (regional states), the DSK. This concept inaugurates a new era of higher fines in data protection.

What was the data protection violation at issue?

According to the Berlin data protection authority's press release, the company in question employed an archiving system to store its customers' personal data, but it was impossible to remove data from the system when the data was no longer required. As a consequence, large amounts of personal data were stored over a lengthy period, even though there was no longer a need to have knowledge of this data. The data included social and health insurance information, employment agreements or information on personal finances, for example. The authority took the view that this constitutes a violation of Article 25(1) GDPR and Article 5 GDPR, which the company failed to remedy, despite an urgent recommendation by the authority to restructure the archiving system.

How was the level of the fine determined?

The first fine in excess of one million euros for data protection violations in Germany comes as no surprise. The supervisory authorities had long announced that there would be more severe penalties. Several weeks ago, they published a draft paper on calculating fines, and this paper was applied in the present case. According to this paper, the annual global turnover of the company that has committed the violation is the starting point for determining the level of the fine. In the case of group companies, this starting point is the turnover of the group. The company is placed in one of 20 classes according to the size of its turnover. For each of these classes based on size, the draft paper sets a flat-rate mean annual turnover, which is then divided by 360 (days) in order to work out a daily rate to calculate the fine. These daily rates range from 972 euros for microenterprises with less than 700,000 euros annual turnover up to 1.25 million euros for a turnover of 450 million euros. For large enterprises with annual turnover exceeding 500 million euros, the daily rate is based on specific turnover figures; one billion euros, for example, entails a daily rate of 2.8 million euros.

In order to determine the fine itself, the daily rate is multiplied by a factor that expresses the severity of the violation. The scale ranges from 1 for minor violations to 12 and above for acts categorized as very serious. The limit for what factor can be selected is set by the fining range provided for in Article 4 GDPR (10 million euros or, if higher, 2% of annual turnover for "formal" violations) and Article 83(5), (6) GDPR (20 million euros or, if higher, 4% of annual turnover for "material" violations).

The supervisory authorities' concept provides for fine-tuning the fine calculated at the end of the process. This fine-tuning covers all circumstances that have not yet been included when assessing the act's severity (e.g. degree of culpability, any earlier violations, as well as the duration of the proceedings or threat of illiquidity).

Focussing on turnover as the basis for determining the fine means that large undertakings will need to expect multi-million euro fines even for comparatively "harmless" violations. To illustrate this, the annual turnover of the company concerned in the Berlin case was around 1 billion euros according to the authority, and this was for an offence of "medium severity".

How should the fine be assessed (in legal terms)?

In legal terms, the calculation of the fine in the present case and the supervisory authority's underlying concept raise a variety of questions. It is strongly disputed, for example, whether group turnover may be taken as the basis where companies belonging to a group have committed data protection violations. Given the enormous fine, of course, the issue of proportionality also arises. It can be assumed that courts will be dealing with these matters in the near future. But some time is likely to elapse before either Germany's Federal Court of Justice or the European Court of Justice has clarified them on the supreme court level. Nor is it a foregone conclusion that German supervisory authorities will be able to push this method of calculating a fine through among their European colleagues. The GDPR provides for a procedure intended to ensure that GDPR data protection rules are implemented in a standard way across Europe. It is quite possible that the European Data Protection Board, which has competence for the matter, will compel the German authorities to make changes that could result overall in both more lenient and stricter fine assessments.

What is to be done?

In the wake of the Berlin data protection authority's decision, it should be clear that fines for data protection violations will be significantly higher in future than to date. This makes it necessary for companies to engage now, intensively, with measures to minimize risk:

- **Data protection compliance:** The best risk minimization strategy is of course to avoid data protection violations in the first place. Even if total data protection compliance is barely feasible, companies should at least have the basic organizational matters on which supervisory authorities focus under control. These include:
  - properly documenting data processing activities within the company (in the form of "records of processing activities")
  - concluding and documenting data protection agreements with all service providers processing personal data on the company's behalf
  - implementing a concept to erase personal data no longer required for any legitimate purpose of processing
  - implementing and documenting data protection impact assessments for "sensitive" processing procedures

- **Awareness of data protection issues:** By now, it should be clear that data protection compliance is a management issue. Company management is responsible for each employee being aware of how important data protection is. This presumes that the company's top management itself is sensitive to data protection issues and is active in furthering data protection compliance (tone from the top).

- **Emergency strategies:** Should a data protection violation be discovered at the company, management will generally need to take action rapidly while keeping a cool head. This will only be possible if the processes and decision-making powers for such an eventuality are clearly defined and known in the company. Cooperation with the supervisory authority is a statutory requirement and generally has a positive impact on the level of fine determined. But this does not mean that the company should prematurely admit that allegations are true or forego measures to defend itself against such allegations. Successful communication with the authority presumes clarity regarding the legal assessment of the incident and thoroughly weighing up the tactical options.

EXPERTISE

Compliance & Investigations
Data Protection
Real Estate

LAWYERS

Dr. Christian Hamann
Dr. Eike Bicker
Dr. Manuel Klar