KNOW-HOW

Gleiss Lutz

01.02.2019

COMPLIANCE & INVESTIGATIONS

EUROPEAN DATA PROTECTION SUPERVISOR: GDPR NOT AN OBSTACLE TO DISCLOSING PERSONAL INFORMATION TO EU INVESTIGATING AUTHORITIES

In a letter to several EU authorities, the European Data Protection Supervisor (EDPS) has commented on an issue that has been worrying compliance departments for months. The date of application of the General Data Protection Regulation (GDPR) in May 2018 and the threat of far tougher fines being meted out for data protection violations have prompted uncertainty among companies as they find themselves confronted with cartel cases, official compliance-related investigations or State aid controls. They wonder whether they are automatically allowed to provide the documents containing personal data, as regularly required by the authorities in these proceedings, without risking an expensive violation of data protection law. This uncertainty apparently reached such a pitch of late that the Data Protection Officers of the European Commission, the European Anti-Fraud Office (OLAF), the European Investment Bank and the European Investment Fund approached the EDPS with the request to clarify the matter. The EDPS, the supervisory authority of the European authorities and institutions as regards data privacy, complied with this request by letter of 22 October 2018.

The key statements of the letter

In summary, the key statements of the EDPS are as follows:

- Compared with the legal situation applying up until May 2018, the GDPR has not changed the rules for companies on the disclosure of personal data to authorities and institutions of the European Union (and of the Member States).
- The EU authorities responsible for regulating competition, combating fraud and controlling State aid are authorised to process personal data within their remit, provided that such is necessary for the performance of their tasks. The legal basis required under data protection law does not emerge from the GDPR but from a data protection regulation specifically for the EU institutions (Regulation (EU) 2018/1725).
- Just as the authorities are authorised to process the personal data required in the performance of their tasks, private companies may likewise disclose these data to the authorities. That applies both in cases where the company is under an obligation to disclose certain information by reason of an explicit statutory regulation or an official order (Article 6(1) sentence 1 (c) GDPR), and in the event of "voluntary" cooperation with the authorities, e.g. whistleblowing or leniency applications in cartel cases. In these latter scenarios, companies may, in terms of data protection law, rely on Article 6(1) sentence 1 (f) GDPR which allows data processing to protect "legitimate interests", provided it is necessary and does not conflict with overriding interests of the data subject.
- It is not compulsory under the GDPR to inform data subjects (e.g. employees) that their data have been disclosed, provided that such data transfer takes place in connection with specific official investigations. Articles 13 and 14 GDPR do specifically provide for data subjects to be informed of the disclosure and the respective recipient of their data. In his letter however, the EDPS refers to the "device" inherent in Article 4 no. 9 GDPR that is intended to avoid an obligation to provide information in the cases referred to here: according to that, public authorities that receive personal data within the framework of a "particular inquiry" in accordance with Union or Member State law are not regarded as "recipients" of such data.
- Nor does the GDPR present an obstacle to arrangements on official audit and control rights in contracts on State aid or the financing of projects with public funds. The authorities do not however act within the framework of a "particular inquiry" in terms of Article 4 no. 9 GDPR. For that reason, companies that in this

- way facilitate authorities' access to documents containing personal data are obliged to inform the data subjects (normally their employees) of the (possible) official measures and the data processing thereby entailed.

Unresolved questions remain

The comments of the EDPS are welcome. They provide clarity, at least on some important points, but do regard matters from the perspective of the (EU) authorities. Material practical issues with which companies are confronted in the context of official investigatory and supervisory measures are not addressed by the EDPS.

- Companies frequently regard one of the main problems as being their obligation to decide which personal data are necessary for the authorities to perform their tasks and may therefore be disclosed. This is only not so in the rare cases where an authority explicitly specifies the documents it requires, at the same time stating whether and to what extent it will accept an anonymization of information. Normally, however, the companies find themselves in a predicament. If they transfer too much personal information they will risk being fined under the GDPR, but if they withhold a sizeable number of documents or blank out large parts of them they may face penalties for their lack of willingness to cooperate, particularly in cases of leniency applications. It would be desirable for it to be made clear on the part of the authorities that companies may withhold, respectively blank out, personal data that are obviously not relevant to the official proceedings concerned, and will only be required to submit them if the authority specifically asks them to do so.
- Particularly in the case of cartel investigations, companies are frequently confronted with requests from the authorities to waive objections to the disclosure of documents and information to foreign cartel authorities. With a view to this practice, the EDPS would do well to make it clear that such a waiver may not relate to personal data that the company has disclosed to an authority. The particular authority alone bears the responsibility for these data and their (further) processing under data protection law. A waiver from the company will therefore not release the authority from its duty to review itself whether the disclosure of data to other bodies at home and abroad is permissible under data protection law. Such waivers will at most make sense where the disclosure of business or trade secrets is concerned.
- Finally, the EDPS's opinion does not deal with scenarios encountered by companies on the question of whether they are permitted to disclose personal data directly to authorities or courts outside of the European Union. The provisions of the GDPR tend to be restrictive but also vague on details. Companies therefore constantly face the dilemma of either risking penalties in third countries for lack of cooperation, or violating stipulations of the GDPR that are punishable with an administrative fine. It would therefore be a great help to obtain clear guidance from data protection authorities on the leeway provided under the GDPR regarding the disclosure of data to authorities in non-EU countries. Ultimately, however, it will only be possible to solve the problems as outlined at the political level by harmonising the international data protection rules and putting practicable mutual legal assistance treaties in place.

This (incomplete) overview is likely to make it clear that the letter from the EDPS of 22 October 2018 is far from solving all problems arising from the conflict between data protection and the disclosure of personal data to public authorities. In many cases therefore, it will still be essential to make a careful analysis of data protection law before deciding on whether or not to disclose documents in official proceedings.

EXPERTISE

Compliance & Investigations

Data Protection

LAWYERS

Dr. Christian Hamann