On February 10, 2020, the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) initiated its first public consultation procedure on the anonymization of personal data, with a particular focus on providers of electronic communication services. As the European Commission Communication in A European Strategy for Data recognized, anonymized data may be used for many purposes and bring enormous benefits to citizens, for example, by improving mobility and road safety.

In its statement, the BfDI reasoned that anonymization, depending on the procedure used, could be a valid alternative to the deletion of data. Expert individuals, stakeholders and companies have until the end of Monday, March 23, 2020, to participate in the consultation procedure. They are encouraged to submit their proposals on the subject of anonymization in light of the General Data Protection
What Is the Purpose of this Consultation Procedure?

Through the consultation procedure, the BfDI hopes to initiate a public debate about anonymization and receive input from the public and affected stakeholders in relation to how the industry is dealing with the subject. The BfDI intends to publish guidance to concerned stakeholders and telecoms providers on the use of anonymization techniques. Interestingly, the guidance will not only be relevant to those that fall into the competence of the BfDI (i.e., telecoms providers and public bodies), but is also anxiously awaited by other industries.

Anonymization Under the GDPR (And the TKG)

Both the GDPR and the TKG refer to the anonymization of data. Pursuant to Sect. 96 para. 3 and 98 para. 1 of the German Telecommunications Act (TKG), a service provider must either anonymize traffic and location data (respectively) or delete them.

Although mentioned in the recitals of the GDPR and directly in the TKG, which transposes the ePrivacy Directive in Germany and thus regulates the processing of traffic data (amongst others), the anonymization of personal data is neither defined nor further described in the GDPR nor the TKG, and remains debated among scholars. Neither the GDPR nor the TKG provide any guidance on how to accomplish this within the framework of the GDPR and TKG.

With lack of a definition, the BfDI utilizes recital 26 of the GDPR, according to which anonymous data is “information, which does not relate to an identified or identifiable natural person,” which is to be determined by taking “all of the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technology developments.”

Furthermore, the BfDI promotes an opinion previously represented in Germany, according to which anonymization should not be construed to mean that absolutely no re-engineering is necessary to ensure that identification is absolutely excluded. However, the BfDI is clear that it believes the re-identification should be so burdensome that no re-identification is feasible because it would be either too costly, time-consuming, or would require too much manpower.

Given that technology is advancing so fast that what is considered anonymous today may not be true tomorrow, it is clear that the anonymization of data requires an ongoing effort by controllers to ensure data stays anonymized. This means it is an ongoing challenge for data controllers to truly anonymize data and maintain technical measures in this regard.

The question remains on how much anonymization is enough. In addition, how much
effort is required of a controller to ensure that data remains anonymized?

**Anonymization And the Need for a Legal Basis**

The BfDI considers that the practice of processing data for the purposes of anonymizing it is a data processing operation that requires a legal basis.

The BfDI proposes that Art. 6 para. 4 GDPR could be an option, which enables the further processing of personal data for compatible purposes, if the new purpose is compatible with the original purpose. Based on Art. 6 para. 1 b) GDPR, the controller could use an Art. 6 para. 4 GDPR balancing test. For example, in cases where customer personal data was processed during the performance of a contract and is now planned to be anonymized to assess services in certain regions by stripping the original data down to only age, place of residence and services bought, the BfDI reasons that the original legal basis could continue to supplement the processing for this new purpose. However, if the purposes are not compatible, this does not answer the question what legal basis would be applicable for the anonymization, **as Art. 6 para. 4 GDPR requires a legal basis, but does not provide one.**

While this might open a door, Art. 6 para. 4 GDPR works only to the extent that future and past processing purposes are compatible, which requires the controller to undergo such assessment.

An aspect not specifically addressed in the consultation is whether Article 6.4 of the GDPR can be used to to further process traffic data.

**COVID-19**

Telecom operators in many European countries have agreed to share traffic and location data to help public authorities fight the COVID-19 pandemic. The guidelines on anonymization may help operators and authorities to ensure that the data is anonymized and its use for mapping the location and spread of the disease, among others.

**Conclusion**

The adoption of this guidance should make it easier for telecommunication companies and for data controllers in general to carry out anonymization, as an alternative to data deletion. In turn, such data may be used for new purposes that may benefit citizens and business in many different ways.

© Copyright 2020 Squire Patton Boggs (US) LLP