Published on *The National Law Review* https://natlawreview.com

German BfDI Initiates Public Consultation Process Regarding Anonymization Under The GDPR

Article By:

Daniel F. Gottlieb

Dr. Claus Färber

The German Federal Commissioner for Data Protection and Freedom of Information (BfDI) recently announced a public consultation process regarding anonymization under the European Union General Data Protection Regulation (GDPR) that is intended to provide the BfDI's position regarding the legal framework for anonymizing personal data and to solicit and evaluate public comments on the topic. The BfDI guidance resulting from the consultation will be helpful since European data protection authorities have not provided any in depth guidance regarding requirements for anonymization under the GDPR.

IN DEPTH

On February 10, 2020, the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) announced a public consultation process regarding anonymization under the European Union (EU) General Data Protection Regulation (GDPR) and, in particular, anonymization within the telecommunications sector. The purpose of the consultation is to provide the BfDI's position regarding the legal framework for anonymizing personal data and to solicit and evaluate public comments. Stakeholders may submit comments to the BfDI through March 9, 2020.

In the announcement of the consultation process, the BfDI focuses on the requirements for determining that data is anonymous data rather than personal data (which includes pseudonymous data) regulated by the GDPR and the need for a legal basis for processing of personal data into anonymous data. Even though the BfDI is the supervisory authority only for telecommunication providers and German federal authorities, the updated BfDI guidance regarding these two matters will be helpful since there is scant direction in the GDPR and from data protection authorities regarding requirements for anonymization. Instead, data controllers and processors often seek guidance from Article 29 Data Protection Working Party (Working Party) opinions under the EU Privacy Directive that were adopted prior to the May 25, 2018 GDPR effective date and are not included among the Working Party opinions adopted by the European Data Protection Board.

Requirements for Anonymization

The BfDI proposes that data may be considered anonymous only when "the personal reference to data has been removed in such a way that it cannot be restored or can only be restored with disproportionate expenditure of time, cost and manpower." The BfDI notes based on GDPR Recital 26 that a data controller must consider the means "reasonably likely to be used" to directly or indirectly identify an individual. While the BfDI sets forth a very high standard for determining that data is anonymous, it is, nonetheless, a lower standard than the absolute zero risk of re-identification standard sought by some privacy advocates.

The BfDI proposal appears generally consistent with Working Party Opinion 05/2014 on Anonymization Techniques, which discusses two options for anonymizing personal data. Under the first option, the data controller may demonstrate effective anonymization by showing that the data set meets the following criteria:

- It is not possible to single out an individual (*e*., distinguish individuals within a group) within the data set;
- It is not possible to link records relating to an individual; and
- Information cannot be inferred concerning an individual.

Where a proposal does not meet the first option's three criteria, the second option provides that anonymization may be based on a thorough assessment of residual re-identification risk. However, the Working Party opinion does not establish any quantitative standard of permissible residual re-identification risk.

Like the Working Party opinion, the BfDI also notes that checking the validity of anonymization is an ongoing task and data controllers should re-assess the risk of re-identification regularly. This is particularly the case due to the rapid growth of computing power and evolution of publicly and privately available data sets.

Legal Bases for Creation of Anonymous Data

The BfDI clarifies that the use of personal data to create anonymous personal data is a personal data processing activity that requires a legal basis under the GDPR. It then proceeds to discuss potential legal bases for the processing of personal data into anonymous data, including the following:

- The valid consent of the data subject;
- Processing for a new purpose (*e.,* anonymization) is compatible with the original legal basis for which the personal data was collected based on the compatibility factors set forth in the GDPR. For example, the BfDI indicates that if personal data is collected for the performance of a service contract with an individual, then the anonymization of the personal data to conduct data analytics to optimize the service for all service recipient may be a compatible purpose; and
- For purposes of erasure of personal data in accordance with an individual's right to erasure under the GDPR.

However, the consultation announcement does not discuss potential legal bases (under GDPR Article 9) for processing sensitive personal data. This omission likely reflects that the consultation process is focused on the telecommunications sector, which typically processes telecommunications traffic data, location data and other personal data that is not sensitive personal data. In addition, the content of the communications would be off-limits under the rules governing the confidentiality of communications.

National Law Review, Volumess X, Number 55