Comments on the document Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

By polypoly GmbH
Country: Germany

Date: 18.12.2019

From a “right of access” to practical access and decision

Enabling data subjects to access and delete their personal information, stored or utilised by companies, is still complicated even though there are legal provisions in the GDPR. Problems stem from poorly defined processes and imprecise formulations.

In the context of article 25 there are two possible approaches that enable data subjects to claim that which is A right following art. 15 GDPR:

1. Companies that process personal data and share that data with other companies, either because it is necessary to process the data for the purpose of fulfilling that service or for other reasons with a purpose not bound to the fulfillment of the service provided to the data subject, should integrate measures that allow the data subject to not only access and potentially send and delete its personal data stored by this first-party-company, but also to reach every third-party company that is involved in the data sharing of the first-party-company tasked with the fulfillment of the service provided to the user.

   The argument follows point 7 of the guidelines and would allow for a “built in” execution of art. 15 while acting as a “safeguard” mechanism protecting individual rights following point 10, which argues for “enabling the subject to intervene in the processing”. This could be as simple as a “request” or “delete” button/field implemented at the website of a company.

2. If this execution of „right by design“ should be rejected, a more precise definition of how to disclose and contact third-party-companies that receive personal data shared by a data processing first-party-company is needed. Every company disclosed needs to be uniquely and exactly identifiable. Right now this is not the case and most of the time it is not clear which exact company truly receives which personal data.

   To solve this the definition needs to include:
   - full name
   - legal form
   - address (country, city, code, street address)
   - register number of the responsible business register (if existing)

Data portability via APIs

Even though data subjects have the right to receive personal data in a machine-readable format, it is still unclear what this means exactly and how this data should be provided. Providing data subjects access to their personal data following art. 15 and 20 via external access APIs that offer comparable latency to the average latency of the internal API used by the company in data processing, would help to further integrate the access possibilities of data subjects. In addition this could shorten the time it takes to process data portability requests and would pave the road for further definitions of the term “machine-readable” with regard to more practical use, processing and analysis of the received personal data by the user and any companies they allow to access it.

Article 25 offers several arguments for implementation:

Chapter 2.1.2 addresses “effectiveness” - point 14 demands controllers be able to “demonstrate” that their measures implement people's rights in a way that they have an actual effect.

APIs for accessing personal data and executing data portability would be a solution that provides scalability, demanded in point 15, and would offer a technical solution to measure key performance indicators and other chosen metrics.

Importantly, however we formulate the need for an implementation of data portability rights via APIs, it is clear that some sort of definition provision needs to be put in place to ensure that these APIs ensure realtime or “close to realtime” access. If this is not the case, implementing an API would be a reductio ad absurdum.

Possibility to control for complete datasets

Data subjects are able to get access to their personal information via art. 15 and 20, but even though companies are obliged to provide complete records, data subjects have no chance of checking that records truly are complete. The consequence is that they may be unable to sue a company for a GDPR infringement because they can’t know if a company is guilty of providing incomplete datasets or if they have truly disclosed all data types collected and companies they share data with.

To be able to make sure of complete data disclosure, data subjects would need to connect with other data subjects and draw large samples of disclosed personal data to ensure that they received a) a complete dataset on their personal data, b) a complete disclosure of what datatypes a company collects and processes, and c) with which companies they share this data.

It is obvious that this is not practical and in itself highly conflicting with the intent of the rights. In order to be able to execute art. 15 and 20. and control for complete datasets, a provision would need to be made, that binds companies to publish the information defined in art. 15 (1) on their data behaviour.

Actual costs of data protection

Differentiating which companies really care about protecting the rights and freedoms of data subjects and defend these principles with an appropriate amount of resources is only possible for technical experts that have insights into those companies. Even though points 23 & 24 give guidelines on the “costs of implementation”of GDPR in general but also the guidelines on art. 25 lack a provision to disclose the “true costs of data protection”.

Requisite spending for GDPR in annual reports and disclosure of the “assessment” mentioned in point 24 should be compulsory for companies. That way data subjects could compare companies with each other and get a better understanding of what effort a company makes and what actions it undertakes to protect their data and their rights. Adding to the “effectiveness” guideline, a standardisation of the naming of the actual costs would help in performing automated analyses. We propose the term “GDPR compliance costs” as the overarching term for the cost summary.

It is clear that this provision could only apply to companies that need to publish annual reports. Small companies often don’t have the possibility and are not bound by law to do so and therefore should not be included in this provision.

Certification for DPbDD - centralised vs. decentralised

With regard to the explanation guidelines for “risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing” in point 28 and what follows, a separation

between centralised and decentralised storage and processing would be of help to clarify the risks posed by different technical approaches for data subjects.

This adds to the overall idea of DPbDD, choosing not only appropriate technical measures, but including the best structures to ensure data protection and the protection of the rights a data subject holds. Because of this, centralised approaches are inherently more likely to pose risks to data subjects rights and the principles in general.