GDPR Webinar 6:
Right to Data Portability

T-Minus 302 Days
(July 27, 2017)

Presenter:
Jeremiah Posedel
Jeremiah.Posedel@dbr.com
@jposedel

DrinkerBiddle

Agenda

- Introduction
- Main Elements of Data Portability
- When Data Portability Applies
- Relationship to Other Rights
- How Portable Data Must be Provided
- Upcoming Webinars
- Q&A

Introduction

Article 20

1. The data subject shall have the right **to receive** the personal data **concerning him or her**, which he or she has **provided to a controller**, in a **structured, commonly used and machine-readable format** and have the right to transmit those data to another controller **without hindrance** from the controller to which the personal data have been provided, where:

(a) the processing is based on **consent** pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a **contract** pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by **automated means**.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal **data transmitted directly from one controller to another**, where **technically feasible**.

Purpose

- Data portability provides the ability for data subjects to obtain and reuse their data for their own purposes and across different services.
- The primary aim of data portability is enhancing individual's control over their personal data and making sure they play an active role in the data ecosystem.
  - Facilitates data subject's ability to move, copy or transmit personal data easily from one IT environment to another.
- Builds on Right of Access

Main Elements of Data Portability

Right to *Receive Personal Data*

- A right of the data subject to receive a *subset* of the personal data processed by a data controller concerning him or her, and to store such data for further personal use.
  - Storage can include a private device or a private cloud.
- Data should be received "in a structured, commonly used and machine-readable format."

Right to *Transmit from One Controller to Another Controller*

- Once received, data subject has right to transmit personal data to another controller "**without hindrance**."
- Data can also be transmitted directly from one data controller to another on request of the data subject and where it is **technically feasible**.
  - Controllers encouraged to develop interoperable formats that enable portability.
  - However, does not create obligation to create systems that are technically compatible.

Disclosing Controllers

- Controllers are not responsible for compliance of receiving controllers.
- However, controllers must ensure that they are acting on data subject's behalf before transmitting data.
  - For example, controllers should establish procedures to ensure that they are transmitting data requested by data subject.
- No specific obligation to check and verify the quality of the data before transmitting it.
- Does not impose an obligation to retain personal data for longer than is necessary or beyond any specified retention period.

Disclosing Controllers (*cont.*)

- When data processed by a data processor, data processing contract must include obligation to assist the controller in responding to portability requests.
  - Includes appropriate technical and organizational measures.
  - Controllers should implement specific procedures in cooperation with its data processors to answer data portability requests.
- Joint controllers should allocate responsibilities clearly via contract.

Receiving Controllers

- Receiving data controllers are not obliged to accept and process personal data transmitted following a data portability request.
- A receiving data controller is responsible for ensuring that the portable data provided are relevant and not excessive with regard to the new data processing.
- Data accepted and retained should only be that which is necessary and relevant to the service being provided by the receiving data controller.

When Data Portability Applies

Covered Processing Operations

- In order to fall under scope of data portability, processing must be based on:
  - Data subject's consent; or
  - A Contract to which the data subject is a party.
- No general right to data portability where processing is based on other basis.
  - Example: Data portability does not cover professional contact details processed in a business to business relationship in cases where the processing is neither based on the consent of the data subject nor on a contract to which he or she is a party.
  - HR data requires a case-by-case approach.
- Data portability only applies if processing is carried out by automated means – most paper files not covered

Personal Data Included

- Data must be:
  - Personal data concerning data subject; and
  - Which data subject ***provided*** to a data controller.
- Anonymous data or data that does not concern data subject is out of scope.
  - HOWEVER, ***pseudonymous data*** that can be clearly linked to a data subject (*e.g.*, by him or her providing the respective identifier) is within the scope.

Personal Data Included (cont.)

- Data ***provided by*** the data subject includes:
  - Data actively and knowingly provided by the data subject (e.g., mailing address, user name, age, etc.)
  - ***Observed data provided by the data subject by virtue of the use of the service or the device*** (e.g., a person's search history, traffic data and location data, heartbeat tracked by a wearable device, etc.)
- Does not include data that are created by the data controller (using the data observed or directly provided as input) such as a user profile created by analysis of the raw smart metering data collected.

Data Concerning Others

- The right to data portability shall not adversely affect the rights and freedoms of others.
  - Intended to avoid the retrieval and transmission of data containing the personal data of other (non-consenting) data subjects to a new data controller in cases where these data are likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects.
- Where personal data of third parties are included in the data set another legal basis for the processing must be identified.
- The processing of personal data by another controller is allowed only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs.
- A receiving data controller may not use the transmitted third party data for his own purposes.

IP & Trade Secrets

- Protection of IP and trade secrets should not lead to a refusal to provide *all* information to the data subject.
- A potential business risk cannot, in and of itself, serve as the basis for a refusal to answer a portability request.
- Data controllers should transmit the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.

Relationship to Other Rights

Other Rights/Obligations

- Data controllers must inform data subjects of the existence of the right of portability.
  - Right must be distinguished from other rights.
  - Also recommended to notify individuals before they close any relevant account.
- Receiving controllers should inform data subjects about the nature of personal data relevant to their services.
- Controllers should verify identity of data subjects exercising right to portability.
- Response to portability request must be ***without undue delay*** ... in any event, ***within 1 month of receipt*** ... but may be extended up to 3 months for complex situations.

Other Rights/Obligations

- If refused, must provide ***reasons*** for not taking action and the ***possibility of lodging a compliant and seeking a judicial remedy***.
- Fee only permitted when requests are manifestly unfounded or excessive.

How Portable Data Must be Provided

Data Form & Format

- Data controllers are expected to transmit personal data in an ***interoperable*** format.
  - However, this does not place obligations on other data controllers to support these formats.
  - Direct transmission from one data controller to another could therefore occur when communication between two systems is possible, in a secured way, and when the receiving system is technically in a position to receive the incoming data.
- Where no formats are in common use for a given industry or given context, data controllers should provide personal data using ***commonly used open formats*** (e.g., XML, JSON, CSV) along with ***useful metadata*** at the best possible level of granularity, while maintaining a high level of abstraction.
- Controllers responsible for take all security measures needed to ensure secure transmission of data.

Upcoming Webinars

Upcoming Webinars

- August 24 – Legal Bases for Processing
  - What are the legal bases for processing of personal data? When is consent a valid legal basis for processing of personal data and what are the conditions for a valid consent? When does the legitimate interest provision apply?
- September 21 – Transparency
  - What information needs to be provided to data subjects? How can we integrate transparency into our day-to-day operations?
- October 26 – Automated Processing and Profiling
  - What are the special requirements that apply to "automated processing" and when do they apply?

Q&A


GDPR 2018