The Scope of EU Privacy Law

BRYAN CAVE

A Broader Perspective℠

When doing business in Europe...

- understand if and to what extent your activities are subject to EU data privacy and security regulation.
- understand your EU business partner is subject to privacy regulation affecting its operations.
- understand the applicable laws and regulation.
- understand how these regulatory requirements affect your business practice.
- understand the legal and commercial risks associated with EU privacy laws.

Scope of EU Privacy law

- The main criteria in determining EU law as the applicable law are the
  - **location of the establishment** of **the data controller**, and
  - **the location of the means or equipment being used when the controller is established outside the EEA**.

- Neither the nationality nor place of residence of the concerned data subjects, nor the physical location of the personal data, are decisive for this purpose.

Scope of EU Privacy law

- EU privacy law (i.e. the national laws of implementation) applies to the processing of personal data outside the EU (EEA):
  - Where it is carried out in the **context of activities of an establishment** in the EEA,
  - as well as to data controllers established outside the EEA when they **use equipment** in the EEA.
- As a consequence, the EU privacy law can be applicable to services with an international dimension such as search engines, social networks and cloud computing.
- Where personal data is processed by a data controller that is not established in the EEA, the processing will fall within the scope of **the national law of any Member State in which equipment (or means) used by the data controller to process the data is located.**
- The criterion ‘use of equipment or means‘ has a broad interpretation, which includes e.g. human and/or technical intermediaries, such as in surveys or inquiries and can go as far as cookies installed on devices located in the EU.

Application of National Privacy Law

- Determine applicable EU national privacy law or national laws.
- Depending on the data processing activity there can be **one national law** applicable **or** even **several national laws**.
- A Member State shall apply its national data protection law where the data processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State.
- When the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

EU Reform Proposal

- Entire EU privacy law concept is subject to significant changes within the next 2 – 3 years.
- Concept of foreign application is planned to be expanded.
- EU Regulation would then apply even if personal data is processed abroad.
- It would apply to all data processing companies that are active in the EU market (e.g. offering goods or services to EU data subjects).

Risk Assessment Factors

- Establishment or legal entity in the EU / EEA
- Data collecting activities in the EU, e.g. surveys, cookies, etc.
- Technical data processing equipment located in the EU /EEA
- Usage of equipment or means located in the EU / EEA for data processing services (servers, hubs, satellite)
- *Business activities in the EU / EEA offering goods or services to EU data subjects*

Indirect Application

- Data Transfer from the EU to countries not ensuring an adequate level of data privacy & security (e.g. U.S. or India)

- EU business partners requesting compliance:
  - due to privacy law requirements applicable to their operation.
  - as part if their operation / compliance strategy.

Data Transfer to the U.S.

- EU data protection law considers the U.S. a country with an inadequate data protection level. This evaluation leads to a **general prohibition of data transfer from the EU to the U.S..**

- To avoid interference with economic needs, several exemptions are regulated to allow such transfer.

Data Transfer Exemptions

- The data subject has unambiguously **consented** to the proposed transfer.
- The **transfer is necessary for the performance of a contract** between the data subject and the data controller or concluded in the interest of the data subject between the data controller and a third party.
- "**Safe Harbor**" certification of the receiving U.S. party, only if transfer itself is lawful by national standards.
- **Conclusion of EU standard terms for transfer of data** (EC L 385/74), only if transfer itself is lawful by national standards.
- Approved **binding corporate rules**.

Consequences of Violation

- National law
- Violation of data protection law could cause different legal consequences. Some examples are outlined below:
  - Monetary Fines
  - Civil claims by data subjects (tort)
  - Civil claims by competitors (in case of interference with unfair competition law)
  - In severe cases even criminal charges

Thank you!

Jana C. Fuchs

Bryan Cave LLP

Hamburg Office, Germany

Jana.Fuchs@bryancave.com

+ 49 (0) 40 30 33 16 136