BREHM & v.MOERS

6 months without Safe Harbor – How to use cloudservices as a European?

Thorsten Rendel (Microsoft)
Kai Bodensiek

BvM more than legal

Personal Data

Art. 2 Data Protection Directive (95/46/EC)

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject');

„**relating information**“ – every information regarding a person, including whereabouts, visits of websites, purchase of goods, download of an app

„**identified or identifiable**“ – it is sufficient that a person may be identified with a reasonable efforts, unclear: IP addresses

Alternativs: anonymize or use of pseudonyms

Statuatory authorisation for data use

- **Consent –** consent has to be given voluntarily (problem: employees) and has to relate to express data and specific uses (problem: informed consent)
- **Fulfilling contractual obligations** – if the use of data is reasonably required for fulfilling contractual obligations (e.g. shipping address, purchase history etc.)
- **Legitimate Interest–** if the data processor has a legitimate interest to use the data but only if the interest of the respective person is not more important (e.g. storing data for system maintenance or security, delivery adress when goods are shipped to a third party).
- Additional authorisations contained in European or national law

Transfer of Data

- **Every transfer of data requires a legal authorization**

- **Alternatives of transfer:**

    - **Controller -> Processor** (contractual data processing)
    - **Controller -> Controller** („real“ transfer including the ownership of the data)

Principle: Unless there is a separate legal authorization an informed consent is always required.

Transfer within the EU

- **Transfer Controller -> Processor:**
  - Legal without consent only if a data processing agreement has been executed
  - Minimum requirements (under German law): subject of the underlying service agreement, scope, subject and purpose of the data processing, category of data and of the respective data subjects, technical and organizational measures for data security, obligations to correct, delete, return or block data, obligation to report violations, right of final decision, right to audit the processor
  - Examples: hosting provider, payroll accounting, SaaS

Transfer to third countries

- For so called secure third countries the same rules as within the EU apply; commission decides on adequate data protection level; currently: Andorra, Argentina, Australia, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, Canada, New Zealand, Switzerland, Uruguay

- **Special case until last year:** USA with Safe Harbor

- **Else only if:**
    - with a valid consent
    - Using „standard clauses“ of the EU-Commission
    - The recipient has implanted binding corporate rules

Valid Consent

- **CONSENT** requires that the data subject is aware of the scope and the impact of the consent and has been fully informed about it („informed consent“). If this is not granted, the consent is void.

- Companies have to inform the data subject on all ACTUAL uses in advance. The information has to be clear without any lack of clarity (negative example: privacy policies of most US major companies that simply try to allow all possible kinds of use).

- The data subject has to be informed about **the specific risks** of the transfer.

- Requirements on clarity and completeness are very high in regard of such consent.

Standard Clauses

- EU-Commission has drafted **standard clauses** that shall secure a sufficient data protection level.
- The standard clauses have to be used without ANY changes, otherwise the data transfer is considered illegal.
- The respective data protection authorities are entitled to forbid a transfer, even if the standard clauses are used, if they reasonably expect that the recipient will not adhere to the standard clauses or that the national authorities will not respect EU data protection principles.

Binding corporate rules

- Recipient has to draft and implement rules for the processing of data including technical and organizational measure for data security.
- This is usually a rather large compliance handbook.
- Those rules have to be approved by the data protection authorities of the data exporter.
- The data exporter is obliged to control compliance.
- In fact this alternative is due to the approval requirements rather rare.

Situation USA

- **Safe Harbor** is according to the judgment of the ECJ void, because US authorities did not grant EU citizens sufficient legal protection and remedy. Furthermore EU data protection principles were not accepted and the Safe Harbor agreement violated the rights of the national data protection authorities because they were not granted any control rights.

- Companies may not claim Safe Harbor privileges anymore since October 6, 2015

- Public authorities are already taking steps against German companies that exported data under Safe Harbor and have not stopped such export

Situation USA – Germany until February 2016

- The conference of the German data protection authorities decided not to take any steps against companies transferring data using individual consent, standard clauses of the commission or binding corporate rules until end of January 2016 but they will not except such export thereafter based on the following considerations:

- **Consent**: in theory possible, but the conference agreed that a sufficient information would require to provide detailed information about the risks of data processing in the USA (including access by public agencies) and that such information is only possible and sufficient in rare cases but anyway not in cases of mass export.

- Employee‘s consent is always not voluntarily because the employee has to fear for his job. This includes transfer to affiliated companies.

- Minors can not grant a valid consent or only in very rare cases.

Situation USA – Germany until February 2016

- **Standard Clauses:** Conference decided that standard clauses are no longer a valid alternative, since the USA do not respect EU data protection principles including legal remedy for consumers. The ECJ expressly stated that the local data protections authorities may decide on that questions.

- **Binding Corporate Rules:** Currently the conference agreed that they will not allow any further binding corporate rule for Export to USA for the same reasons.

- **Consequence: With some rare exceptions, currently any transfer of personal data to the USA in illegal in Germany. Cloud services for personal information that use servers in the US or allow US employees to access such servers are in violation of German data protection law.**

Situation USA – March onward

- **PRIVACY S.H.I.E…..SHIELD*:** US and EU authorities have announced that they reached an agreement on a new cooperation model, that is now called Privacy Shield. Meanwhile first drafts of a general data export agreement and of the Privacy Shield agreement have been published.

- While Privacy Shield contains significant new rules on the oversight of the data protection rules and for the first time actual reviews have become mandatory, most other parts are very similar to Safe Harbor.

- No guarantees that are liable in court will be granted in regard to access to personal data by security agencies, only a „statement“ is provided.

- *** SCNR**

Situation USA – March onward

- Just last week the Article 29 Working Party (a group consisting of the EU data protection authorities whose rights have been significantly strengthened by the ECJ) has published a harsh statement regarding the lack of clarity of the Privacy Shield provisions. The drafts use a different wording that the EU data protection provisions and do make clear that those EU principles are to applied.

- The Working Party criticized the lack of provisions in regard of the purpose limitation principles (data may only be used for the purpose it has been collected for) as well as a clear system of legal remedy and venue in the draft.

- Last but very important is that the Working Group does believe that the “statement” regarding the massive collection of personal data is sufficient and will not accept such a low level of disclosure by the US authorities.

Breach

- **Unauthorized Use:** fine of up to 350.000 Euro; in individual cases higher in order to collect profits
- **Commercial unauthorized use** : criminal charge (board members and directly involved employees): prison of up to 2 years or a fine.
- **Cease and Desist** from data subjects and consumer protection agencies
- **Negative Publicity**

What can we do until there are new rules?

Thorsten, what will Microsoft and the other cloud service providers do in the meantime to resolve this issue?

BREHM & v.MOERS

Thank you for listening!

Kai Bodensiek
Rechtsanwalt

Anna-Louisa-Karsch-Str. 2
10178 Berlin

Tel.: 030 – 26 93 950
Fax.: 030 – 26 93 95 15

Kai.Bodensiek@bvm-law.de
www.bvm-law.de