Data Governance and Data Protection in the context of Cloud Services

GWF2021: Tech Session: 5G, Cloud & IoT
22 October 2021 | Gerhard Deiters and Philip Lüghausen, Lawyers, BHO Legal
What is Data Governance?


- “Data governance is a term used on both a macro and a micro level”
- “On the macro level, data governance refers to the governing of cross-border data flows by countries, and hence is more precisely called international data governance. This new field consists of “norms, principles and rules governing various types of data.”
- On the micro level “data governance is a data management concept concerning the capability that enables an organization to ensure that high data quality exists throughout the complete lifecycle of the data, and data controls are implemented that support business objectives”

Here, we want to focus especially on two aspects: Data Ownership and the draft (!) EU Data Governance Act
Data Ownership

- You can own a property, car, laptop, smartphone etc
- But can you own data?
- At least in most of the European jurisdictions, there is no such concept as „Data Ownership“
- Thus, geospatial data collected and processed by companies requires legal or contractual protection other than the concept of ownership
  - It seems logical at first to compare geospatial data with software and assume a copyright
  - However, it must be taken into account that geospatial data is not an individual intellectual creation
  - Image recordings may enjoy copyright protection under certain circumstances
  - Data sets may constitute a database in certain circumstances and be subject to the sui generis right of the EU Database Directive
  - In principle, however, there is a risk that valuable geospatial data are not subject to any legal protection and can therefore be freely used by third parties
Data Ownership

→ Data “owners” must therefore protect themselves through licences against their valuable data being used and disseminated by third parties without benefiting themselves.

→ Such licences have a completely different purpose than classic software licences:
  → The user of a software requires a licence in order to be allowed to use the software.
  → In the case of data licences, on the other hand, the licence must restrict the rights of the user in order to protect the party providing the data.

→ In the context of cloud services, protection must strictly speaking not only be agreed with the purchasers of the data, but also with the operator of the platform.

→ Unlike copyright protection, the data licence does not have absolute effect (i.e. vis-à-vis everyone), but only relative effect between the contracting parties.
On 25 November 2020, the European Commission published a proposal for an EU Data Governance Act.

The draft EU Data Governance Act addresses the following situations:

- Making public sector data available for re-use, in situations where such data is subject to rights of others.
- Sharing of data among businesses, against remuneration in any form.
- Allowing personal data to be used with the help of a ‘personal data-sharing intermediary’, designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR).
- Allowing data use on altruistic grounds.

The draft EU Data Governance Act does not establish a concept of Data Ownership.
However, the draft EU Data Governance Act establishes a lot of obligations on private “data sharing service providers” (the following list is only an excerpt):

- The service provider of data sharing services who intends to provide services shall submit a notification to the competent authority.
- The service provider of data sharing services that is not established in the EU, but offers services within the EU, shall appoint a legal representative in one of the Member States in which those services are offered and the provider shall be deemed to be under the jurisdiction of the Member State in which the legal representative is established.
- The service provider may not use the data for which it provides services for other purposes than to put them at the disposal of data users and data sharing services shall be placed in a separate legal entity.
- The service provider shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data holders and data users, including as regards prices.
- The service provider shall facilitate the exchange of the data in the format in which it receives it from the data holder and shall convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by EU law or to ensure harmonization with international or European data standards.
The service provider shall have procedures in place to prevent fraudulent or abusive practices in relation to access to data from parties seeking access through their services;

The service provider shall ensure a reasonable continuity of provision of its services and, in the case of services which ensure storage of data, shall have sufficient guarantees in place that allow data holders and data users to obtain access to their data in case of insolvency;

The service provider shall put in place adequate technical, legal and organizational measures in order to prevent transfer or access to non-personal data that is unlawful under EU law;

The service provider shall take measures to ensure a high level of security for the storage and transmission of non-personal data;

The service provider shall have procedures in place to ensure compliance with the Union and national rules on competition;

The service provider offering services to data subjects shall act in the data subjects’ best interest when facilitating the exercise of their rights, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses;

Where a service provider provides tools for obtaining consent from data subjects or permissions to process data made available by legal persons, it shall specify the jurisdiction or jurisdictions in which the data use is intended to take place.
Dealing with Personal Data within the EU requires GDPR compliance

WHY DO YOU GET THAT LOOK WHENEVER WE TALK ABOUT GDPR COMPLIANCE?

© marketoonist.com
Data protection and the "5 stages of grief"

1. Denial: it can't be true!
   - We don't process personal data

2. Anger: who did this to me?
   - The evil EU
   - Unworldly desk jockeys

3. Negotiate: How can I make it up to you?
   - There must be a simple solution

4. Depression: I can't turn it away!
   - It is difficult or impossible to make up for omissions retrospectively

5. Acceptance: I accept the situation
   - Okay, I'm setting myself up for the future...
Data protection in the context of Cloud Services

➔ If we are dealing with companies or public bodies in the EU, we have to take into account the „infamous“ GDPR

➔ The GDPR lays down rules relating to the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data

➔ If you offer geospatial data via cloud services within the EU and EEA, the regulations of the GDPR must be observed

➔ But now stop for a while, geospatial data is information about geographic locations that can be stored in and used with a geographic information system

➔ In the context of geospatial data, we do not even want to process personal data...
We do not process any personal data...
We do not process any personal data...

https://www.google.com/maps/place/Blessem,+50374+Erfstadt/@50.8141885,6.7944829,135m/data=!3m1!1e3!4m5!3m4!1s0x47bf16291a3dc5e3:0xa2760fee1eb07d0!8m2!3d50.8132732!4d6.7966581
Possible information among others:
- Condition of the land
- Loss of value
- Pollution
- ...

Interesting for insurance companies?

Level of detail may reveal further information
First Conclusions

- Personal data are also regularly processed in the area of geospatial data, regardless of whether this is intended.
- Personal data can
  - be contained in photographic material itself
  - be "created" by linking with other information
  - arise in the course of processing (employees, third parties)
- Therefore, we must assume to be in the scope of the GDPR for the time being.
- But that's no drama, because data protection is not witchcraft.
- Basically, the GDPR obliges us to adhere to the following principles:
  - Collection of data only for specified, explicit and legitimate purposes ("purpose limitation")
  - Processing in a lawful and comprehensible manner ("lawfulness & transparency")
  - Limitation of processing to what is necessary ("data minimisation")
  - Storage only as long as required by the purpose of the processing ("storage limitation")
Currently, there is general uncertainty among companies regarding the question as to what measures must be complied with for international data transfers.

This relates primarily to the publication of the ECJ decision "Schrems II" (Case C-311/18), which declared data transfers to the USA solely based on the EU-US Privacy Shield to be illegal.

It concerns all data transfers from/to the EU and in particular those data transfers that cannot be based on a so-called adequacy decision of the EU Commission (as they exist, for example, for Japan and the UK) or other exemptions, such as in Article 49 GDPR.

So, if e.g. you are a service provider outside the EU and the EEA offering services to companies with the EU or if you are contracting a subcontractor outside the EU and EEA to offer your services, you might be obliged to use the new set of the so-called Standard Data Protection Clauses, or Standard Contractual Clauses adopted and published by the European Commission on 4 June 2021 (https://t1p.de/0dym).
BHO - Baumann Heinrich Ortner
Rechtsanwälte und Patentanwalt Partnerschaft mbB
Hohenstaufenring 29-37 | 50674 Cologne

Gerhard Deiters
Lawyer | Partner
Fon +49 (0) 221 270 956 160
Fax +49 (0) 221 270 956 222
gerhard.deiters@bho-legal.com
Dr. Philip Lüghausen
Lawyer | Partner
Fon +49 (0) 221 270 956 210
Fax +49 (0) 221 270 956 222
Philip.lueghausen@bho-legal.com