Law | Policy Concepts

PC.24 Data Trust

Authors: Louisa Specht-Riemenschneider, Jakob Knapp, Aline Blankertz

Last update: 2021-06-25 07:23:20 | By: Louisa Specht-Riemenschneider

Created at: 2021-05-16 11:06:33

A data trust is

> *"a natural or legal person or a partnership that mediates access to data provided or held by data trustees in accordance with contractually agreed and/or legally prescribed data governance regulations in the interests of third parties."*

[*Specht/Blankertz et al.*, Die Datentreuhand, MMR-Beilage 06/2021, p. 25 ff. with further references].

This may include Personal Information Management Systems (PIMS), data rooms, data hubs, data lakes, data escrows, etc. The element of safeguarding third-party interests, which gives the data trust its fiduciary character, is decisive. The functionality of providing access to the data is central. Other functions of the data trust can of course be added, for example:

? Pseudonymisation and/or anonymisation of data

? Decision on the access of third parties to the data

? Data evaluation

There are four basic forms of data trusts, which differ in terms of the centrality and decentrality of data storage as well as the voluntary or mandatory use:

	Voluntary	**Mandatory**
Decentralised Data Storage	Voluntary Data Cache	Mandatory Data Cache

Centralised Data Storage	Voluntary Data Host	Mandatory Data Host

The use of **voluntary data trust models** is based on the willful decision of the parties involved, in particular the data subject or the technical-factual data holder. In this process, the parties conclude a data trust agreement which becomes the basis of the legal relationship. Voluntary models are conceivable, for example, for the state agricultural data platform envisaged in the **Data Strategy of the German Federal Government**, for biodatabases, for the sharing of hospital data for research purposes **[see also Tile P.12]** or for the creation of a "circular data space" for digital product passports.

The **voluntary data cache** is a voluntarily deployed data transmission instance that, for example, makes the data access decision according to legally or privately autonomously prescribed access conditions. It is conceivable, for example, that clinics keep data locally and that these are released by a trust in order to temporarily enable the training of algorithms.

A **voluntary data host**, on the other hand, stores the data centrally. An example - if they store data centrally - are PIMS **[Tile PC.40]**. They may grant the data subject access to data stored about them if they exercise their data subject rights. In the case of consent management, they may provide third parties with access to data of the data subject. Data escrows also belong to the category of optional data hosts.

Mandatory data trust models, on the other hand, are characterised by the fact that technical-factual data holders are legally obliged to use the data trust in certain processing situations or to outsource their data to the data trust altogether. This can be an important solution especially for those cases where the technical-factual data holder is not the (only) legitimate data holder. An example of a mandatory data host is the data trustee proposed in the mobility sector by the German *56th Verkehrsgerichtstag*, where the data from the accident vehicle is stored **[Empfehlung des Arbeitskreises II, Ziffer 5]**. But the cancer registry is also such a mandatory data host. Sometimes it may be necessary to store data centrally with a data trustee in order to exclude the person processing the data from access (see Microsoft Cloud).

Mandatory data cache models (data pass-through entities) can be found in the **Australian Consumer Data Right** with the Gateway Person.

What is largely non-existent so far are **voluntary data trust models organised under private law** that allow e.g. researchers to share their data with each other in a secure environment under the legal requirements (one of the few examples of use is service of the company **Apheris**) **[see also Tile CO.14]** . They are necessary because previous trust models, such as the cancer registry, are limited to certain data. Only voluntarily created data spaces allow flexibility in the type of data shared. For example, radiology image data could be shared for research purposes in such a voluntary data trust. Such data trust models should be regulated on an incentive basis [*Specht/Blankertz et al.*, Die Datentreuhand, MMR-Beilage 06/2021, p. 25 ff. with further references].