Use cases from the perspective of Deutsche Telekom's Group Privacy

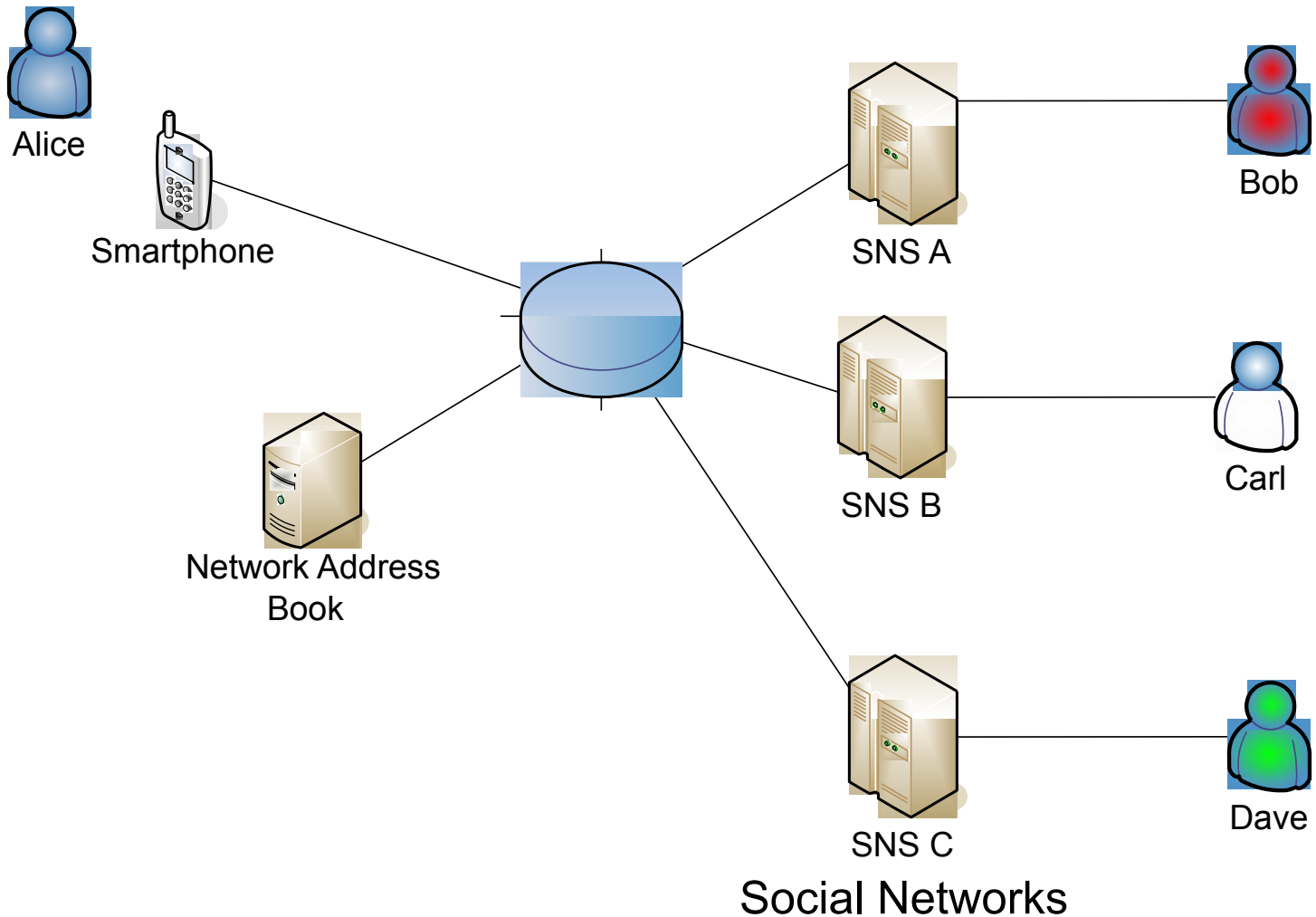
W3C Workshop on Privacy and data usage control

Life is for sharing.

Synchronizing address information from social networks Description

- One of our products lets users synchronize contact information from various sources (e-mail client, cell phone, etc.) with an address book on the Internet.
- A function has now been added to this product that allows data from address books on social networking sites to be synchronized, too.
- The exchange of data is legitimized by the user, who is also a user of a social network.
- Framework conditions are also defined via technical parameters (APIs) and legal parameters (terms & conditions).

Synchronizing address information from social networks Representation



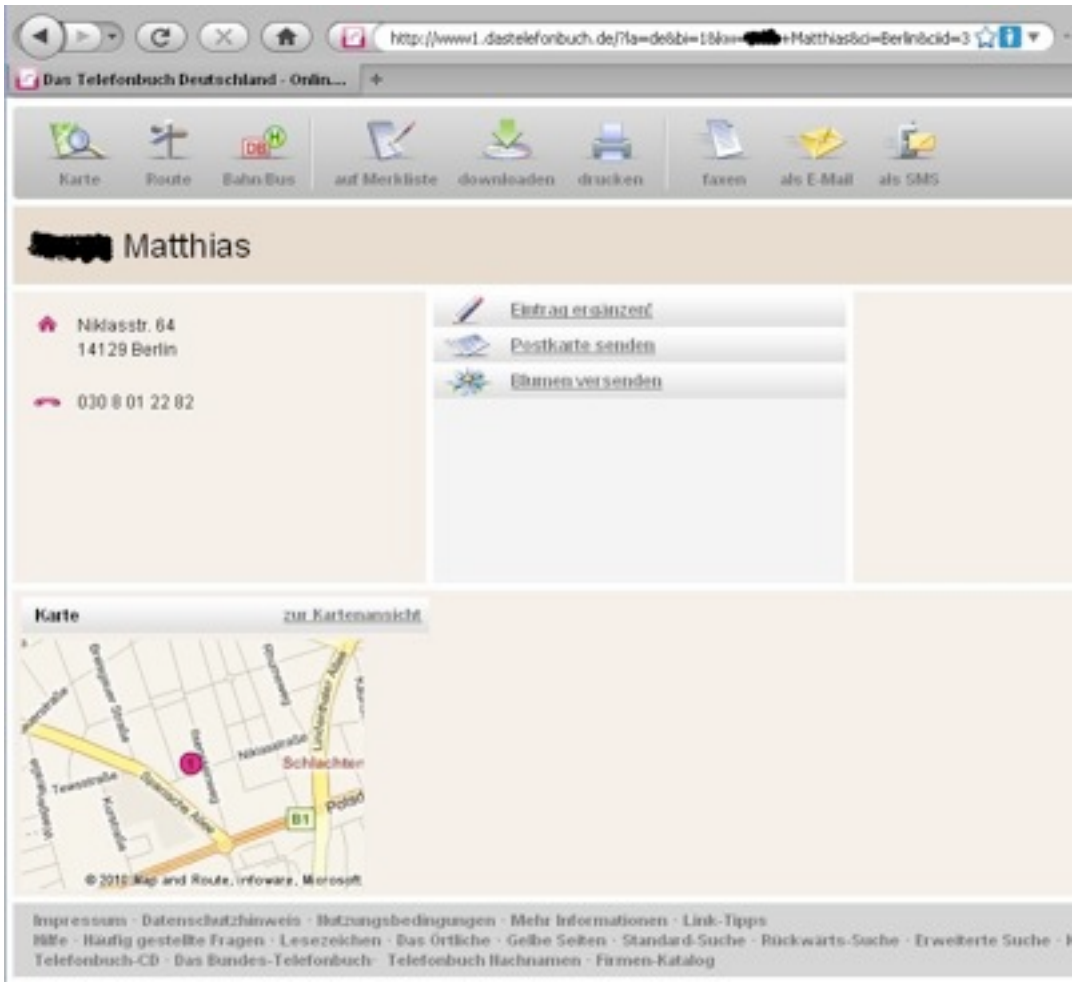
Synchronizing address information from social networks
Open issues, challenges

- The following situations may arise after legitimized synchronization of released address details from the social network to Alice's network address book:
  - Change of details relating to existing relationships (Bob has a new telephone number)
  - New details relating to existing relationships added (Bob now also has a Skype account)
  - New details relating to new relationships added (Carl is now also Alice's buddy)
    - ➔ no (new) problems, but what happens when:
  - Existing relationships are canceled (Dave is no longer Alice's buddy)
  - Under certain circumstances Alice may still keep Dave's details against Dave's wishes
  - Are there solutions that can guarantee Dave "sovereignty" over his details?
  - How can the use of these solutions be ensured on the market?

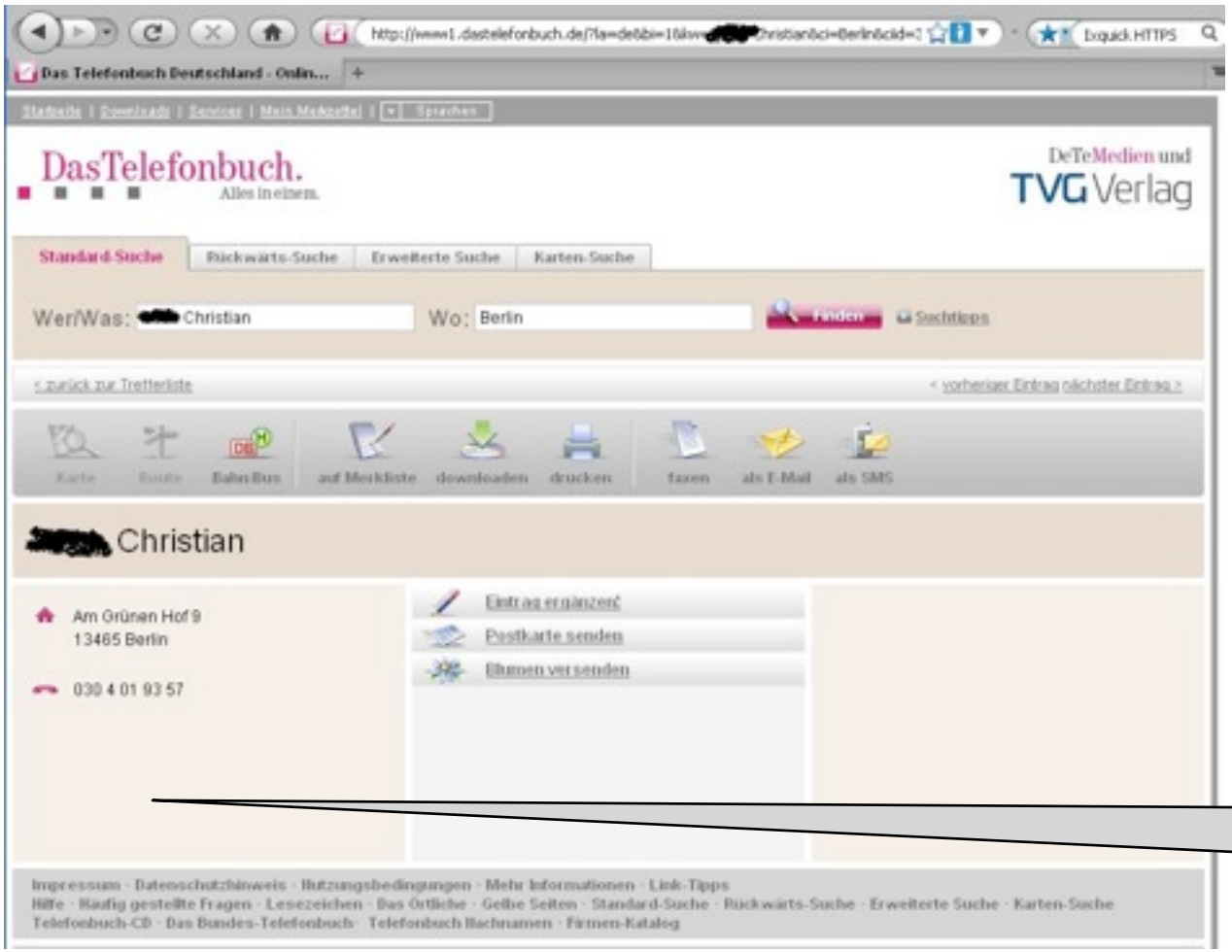
Linking phonebook entries with geodata

- Online phonebooks link addresses with city maps as well as satellite and aerial photos if customers do not object.
- In keeping with this right to object, customers are offered the opportunity to deactivate direct links within the portals.
- Effective protection against disclosure of the address in the relevant map material on the Internet could only be provided by refusing publication of the address in all public telecommunications directories. Depending on the individual needs of the customer, this is not always an adequate solution.
- In general, there is no easy way to block access to map material in the case of well-known addresses. It's always possible to find well-known addresses via other Internet services (Google maps, bing maps, route planners).

Linking phonebook entries with geodata
Standard scenario - no objection

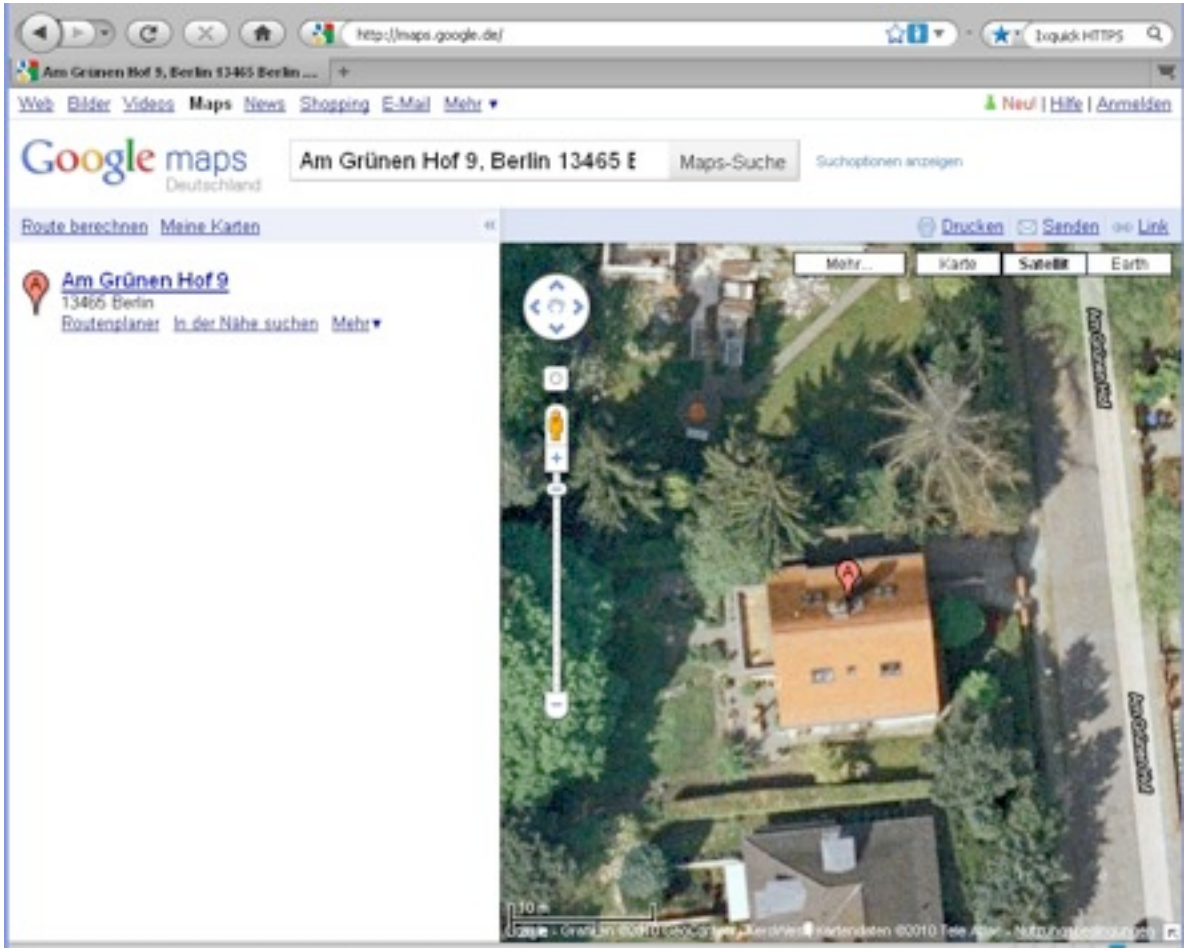


Presentation when customer objects



No link to map material

Linking of telephone directory entries with geodata manual search for the address previously found



Linking phonebook entries with geodata
Current discussion in Germanyscenario

- There is currently widespread public debate in Germany about Google Street View and other mapping services that make houses and entire streets accessible on the Internet via both satellite imaging and aerial photos.
- Google has made far-reaching concessions to the German data privacy authorities. Homeowners have the option of blocking publication of Street View images on the Internet.
- This is not yet covered by legislation in Germany.
- In the course of the debate about the potential requirements of additional legal regulation, the German Minister of the Interior called upon the Internet sector to introduce self-regulation of the handling of new Internet services by December.
- The aim of this self-regulation would be to establish a general right to object to the publication of geo-referenced personal data on the Internet.

Linking phonebook entries with geodata
Open issues, challenges

Irrespective of open issues that can or should be clarified as part of this workshop, such as:

- Do houses that are visible on aerial photos fall under personal data?
- How can an objection be legitimized?
- How can national laws be applied to international services or the Internet?

... the following questions have to be addressed:

- Are solutions based on the assumption of a central database of all objections being in the hands of a single trusted party feasible and workable?
- Are there technologies that can allow/forbid an inquiry relating to a certain address depending on a legitimization (e.g. fulfillment of the condition "no objection filed for the requested address")?
- Under what preconditions can solutions be realized independently of the provider of the mapping material?

Access to data in last level support
IT factory in telecommunications in Germany

The processing of personal data, the content of calls and the immediate details relating to telecommunications are the subject of a dedicated law in Germany.

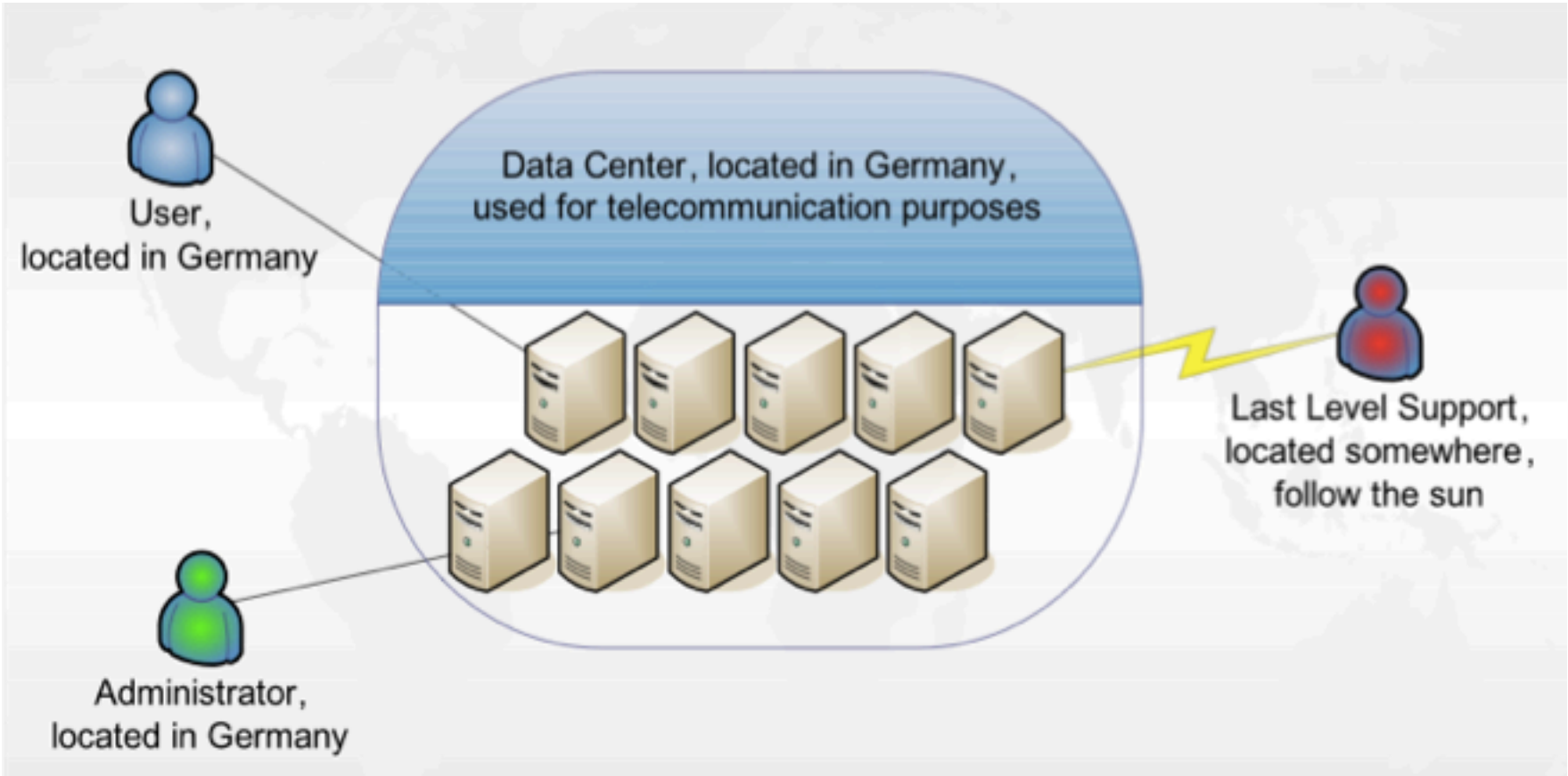
In addition to the handling of customer data and detailed measures to ensure observation of the fundamental right to the confidentiality of communication, this law also specifies the framework conditions permissible for the processing of data.

Under the provisions of this law, telecommunications data may not be processed outside of Germany. Exception: Data has to be processed for telecommunication or its billing. This relates to international telephone calls, for example.

International outsourcing, for example for cost reasons, is forbidden by this provision.

Also forbidden are remote access to data, as even displaying the data on a monitor abroad represents transmission within the meaning of German data privacy law.

Access to data as part of last-level support
Sample presentation



Access to data as part of last-level support
Description of problem

The diagram shown on the previous page for illustration purposes describes a typical part of IT at Deutsche Telekom. In the example shown, telecommunications data is to be processed. Let's assume bills are to be generated for customers in Germany.

Call data records are analyzed according to the calling plan the customer has selected and are then summarized in a bill.

The underlying infrastructure consists of IT applications created specially for this purpose. These applications were partly developed for Deutsche Telekom by external companies. The infrastructure consists of databases, storage, processors - everything you would find in a typical data center.

All the well-known German and international manufacturers are represented in terms of the equipment in the data center. Support agreements have been concluded with all of them in case of problems.

The vast majority of manufacturers offer last-level support according to the "follow the sun" principle. Depending on the amount of work involved, ongoing trouble tickets may span the globe.

Access to data as part of last level support
Open issues, challenges

- Access is global.
- Access rights are so broad that access to data on the system in question cannot be ruled out.
- But access is only permitted from within Germany.

Question:

- What technical possibilities are there for allowing worldwide access in the scenario described, while at the same time preventing the transmission of the data to be processed from being transmitted to undefined places outside of Germany?

Note:

- Similar solutions are needed in the field of cloud computing to be able to make use of the potential flexibility while observing the conditions of (German) data privacy laws...

Thank You.

frank.wagner@telekom.de

Life is for sharing.