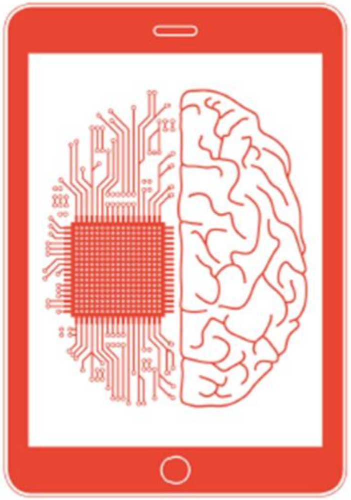
University of Applied Sciences and Arts Northwestern Switzerland
School of Life Sciences



# Patient-Centric eHealth Data Exchange Using Distributed Ledger Technology

Master Thesis MSc Medical Informatics

Nico Heiniger

dHealth Network

# Agenda

- **Research problem and motivation**
- **Approach to the problem solution**
- **Software architecture**
- **Prototype demonstration**
- **Results**
- **Conclusion**
- **Q & A**

# Research Problem and Motivation

## Patient side

- Smart watches / wearables track heartrate and sleep rhythm
- Fitness apps track nutrition and workout data
- General practitioner visits generate data (blood tests, medical history)

→ Large amount of data created

## Researcher side

- Artificial intelligence and machine learning to discover new drugs or predict patient outcome
- Prediction models need large amounts of data
- Data collected in clinical trials is expensive and can deviate from real-world setting

→ Large amount of data (RWD) needed

# Research Problem and Motivation

***What are the technical possibilities for designing a platform to share health data between patients and researchers?***

# Approach to the Problem Solution

## Analysis of stakeholders and their core requirements

- Patient: Data Privacy & Transparency
- Research: Data Quality & Integrity and Performance & Efficiency
- Care Provider: not in focus

## Objectives

# Objectives

## Data Privacy & Transparency:

- The patient can see where their data has been sent.
- The patient can control whom they share their data with.
- The applicable data protection laws need to be followed.

## Data Quality & Integrity:

- The data needs to be in machine-readable format.
- Meta-data is available.

## Performance & Efficiency:

- Access to data should be fast (number of transaction per second > 60).
- Response time should be acceptable (loading times < 4 seconds).

# Methodology

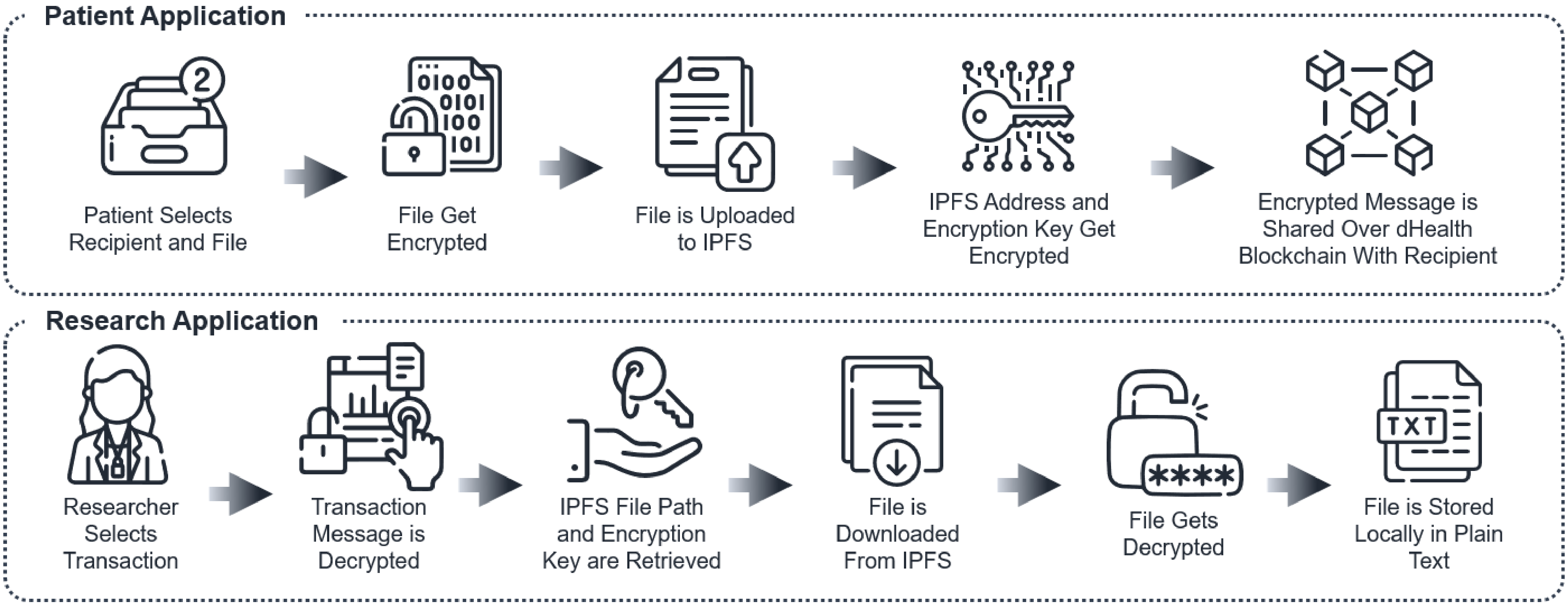
- **Minimum viable product (MVP) → proof-of-concept**
- **Blood sample data (laboratory results)**
- **Build a prototype using dHealth blockchain**
- **Evaluate prototype based on own objectives and requirements from existing frameworks**

# Software Architecture

**Technology stack used:**

- **TypeScript and Node.js in Visual Studio Code**
- **HL7 file format**
- **AES-256 encryption algorithm**
- **dHealth network as blockchain for the data exchange**
- **IPFS network as a distributed data storage**

# Software Architecture: Process



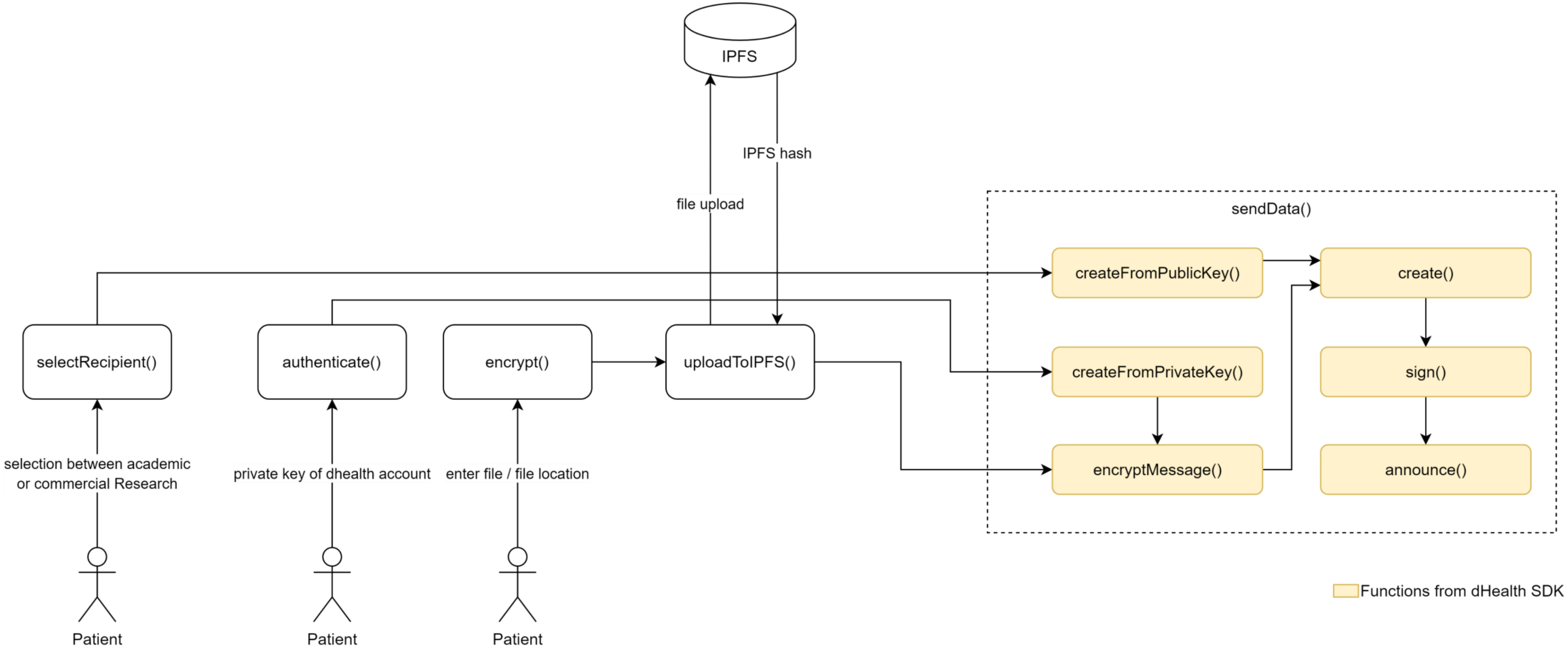
Patient Application

Patient Selects Recipient and File → File Get Encrypted → File is Uploaded to IPFS → IPFS Address and Encryption Key Get Encrypted → Encrypted Message is Shared Over dHealth Blockchain With Recipient

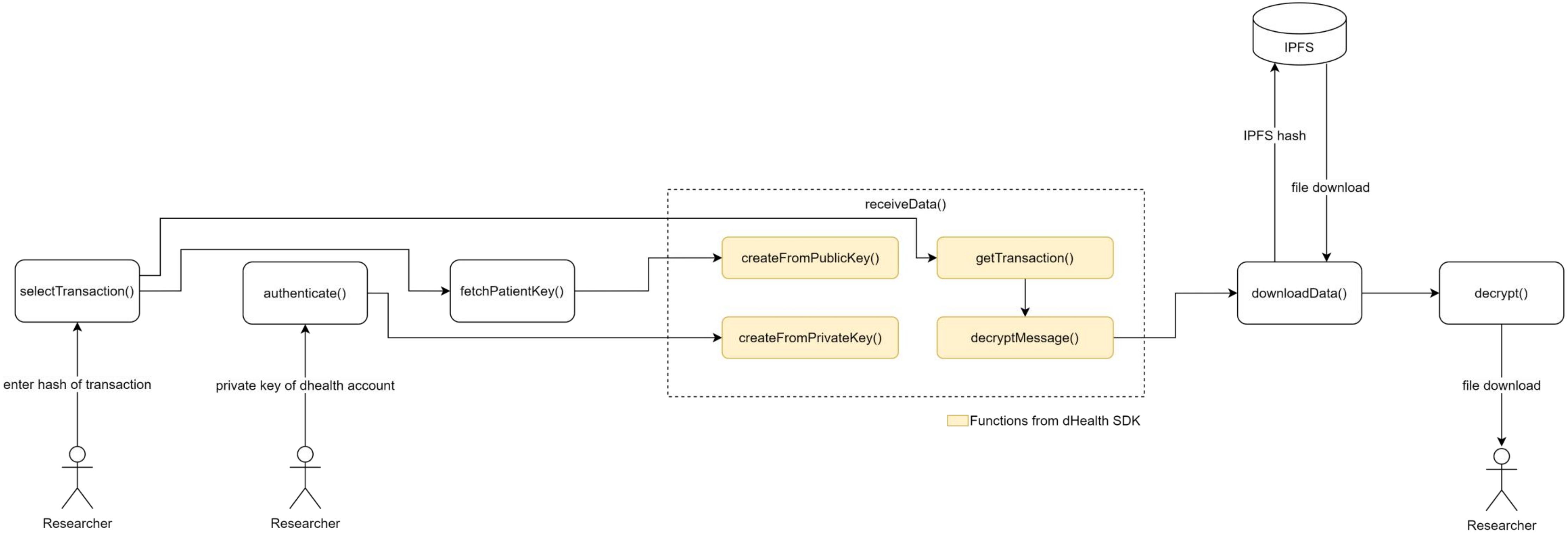
Research Application

Researcher Selects Transaction → Transaction Message is Decrypted → IPFS File Path and Encryption Key are Retrieved → File is Downloaded From IPFS → File Gets Decrypted → File is Stored Locally in Plain Text

# Software Architecture: Patient Application



# Software Architecture: Research Application



# Prototype Demonstration

# Results

- **Working prototype using dHealth and IPFS**
- **Prototype covers Data Privacy, Data Quality and Performance objectives almost fully**
- **91% of requirements are covered by default or with organisational extension**
- **Performance and cost suggest scalability**
  - Transactions per second: 60
  - Annual transaction fees: around 4000 CHF

# Results: Objective

## Data Privacy & Transparency:

- The patient can see where their data has been sent. ✓
- The patient can control whom they share their data with. ✓
- The applicable data protection laws need to be followed. !

## Data Quality & Integrity:

- The data needs to be in machine-readable format. ✓
- Meta-data is available. ✓

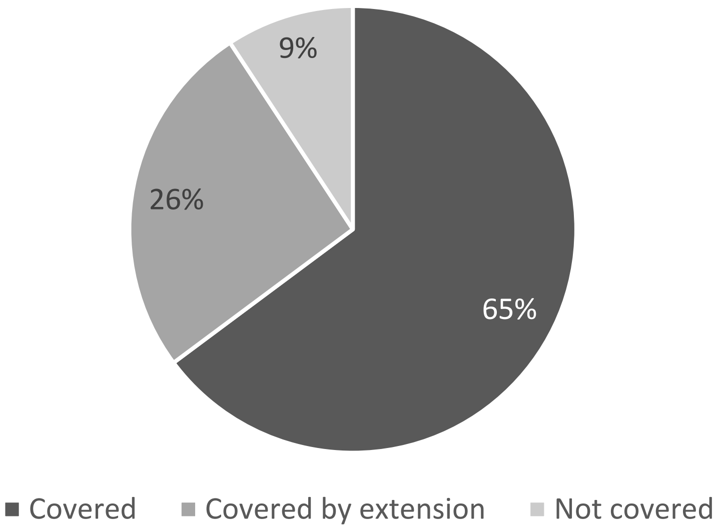
## Performance & Efficiency:

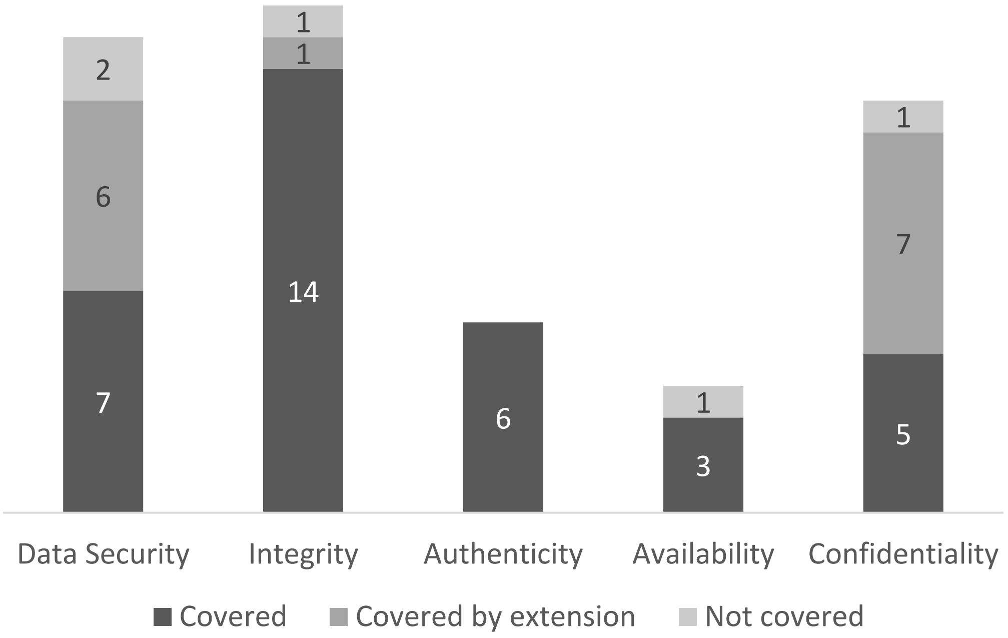
- Access to data should be fast (number of transaction per second > 60). ✓
- Response time should be acceptable (loading times < 4 seconds). ✓

xception: Data deletion & access logs

# Results: Requirements

## 91% of requirements are covered by default or with organisational extension





# Results: Data Deletion in Theory

## GDPR Chapter 3, Art. 17:[1]

**The right to be forgotten:** Individuals have the right to ask for the complete deletion of their personal data with an organisation. In such a situation, the organisation is also obliged to notify any third parties with whom the data was shared.

[1] https://gdpr-info.eu/art-17-gdpr/

## Results: Data Deletion in Reality

- **Deletion occurs when it is no longer possible for anyone to recognize the information in question without disproportionate effort.**[1]
- **In previous rulings by the European Court of Justice a "sufficient deletion" was the failure to display certain information.**[2]
- **The obligation to delete does not include copies made by third parties to whom the data has been shared.**[3]
- **In this case, only the data controller's notification obligation apply.**[3]

[1] Herbst, T. (Ed.). (2020). Art. 4 Nr. 2 DS-GVO N 36. In Datenschutz-Grundverordnung, BDSG: Kommentar (3. Auflage). C.H. Beck.
[2] Google LLC vs CNIL. (2019) / Google Spain vs AEPD. (2014).
[3] Herbst, T. (Ed.). (2020b). Art. 17 DS-GVO N 41. In Datenschutz-Grundverordnung, BDSG: Kommentar (3. Auflage). C.H. Beck.

# Conclusion

- **Data sharing / donation is technically feasible**
- **High level of trust of blockchain technology through immutability, transparency and security**
- **High availability and integrity through distributed storage network**
- **Most likely GDPR requirements are covered, further legal clarification needed**
- **Further research should be done into other encryption methods, aggregate transactions and the economical perspective**

# Q & A