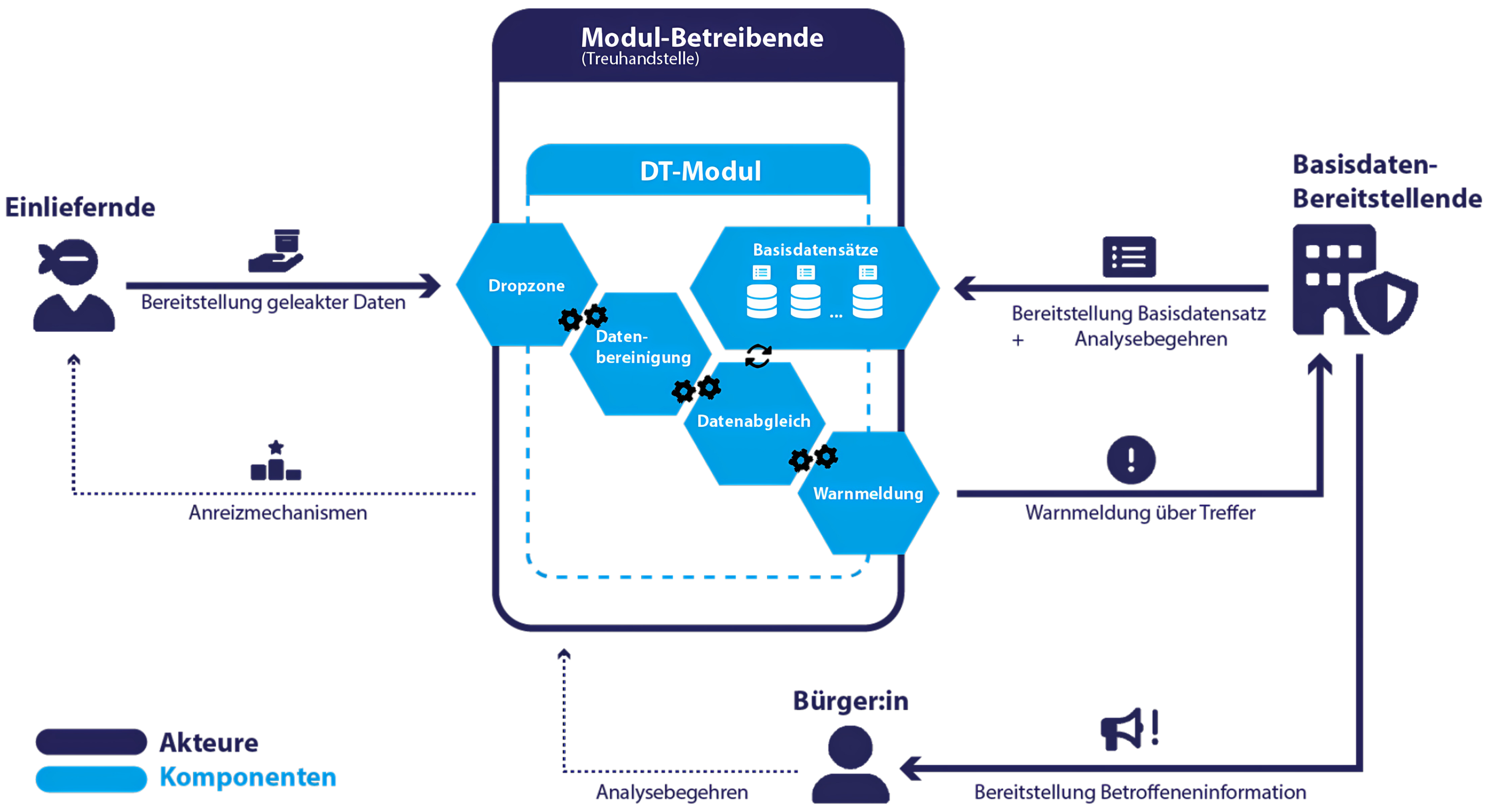
Institute for Information- and Economic Law (IIWR)
Centre for Applied Legal Research (ZAR)
Computer Science 4 (UBO)

DROPS – Data Escrow Module For The Preventative Protection Of Identity Data Against Misuse

Funding of projects for the research or development of practically applicable solutions (‘building blocks’) for data escrow modules

Franziska Boehm, Florian Idelberger, Stephanie von Maltzan (KIT) | Michael Meier, Marc Ohm, Daniel Vogel (UBO)

The main goal of the work package Data intake and incentive mechanisms is the development of a technologically feasible data intake mechanism, while taking account of legal requirements. This mechanism should allow for the intake of structured and unstructured data and incorporate an incentive mechanism that incentivizes whistleblowers or security researchers to submit data to the DROPS module. Additionally, we present a secure interface to compare between submitted data and user supplied data. The project especially took account of legal requirements and the protection of whistleblowers. The development of the data intake mechanism is based on extensive analysis and research of the legal environment and the technical possibilities. These analyses considered existing technologies as well as innovative new approaches such as small local AI models, to develop a flexible and robust solution. A significant hurdle during past work and for further development is the variety of possible file and data formats that have to be supported, while maintaining security and privacy guarantees.



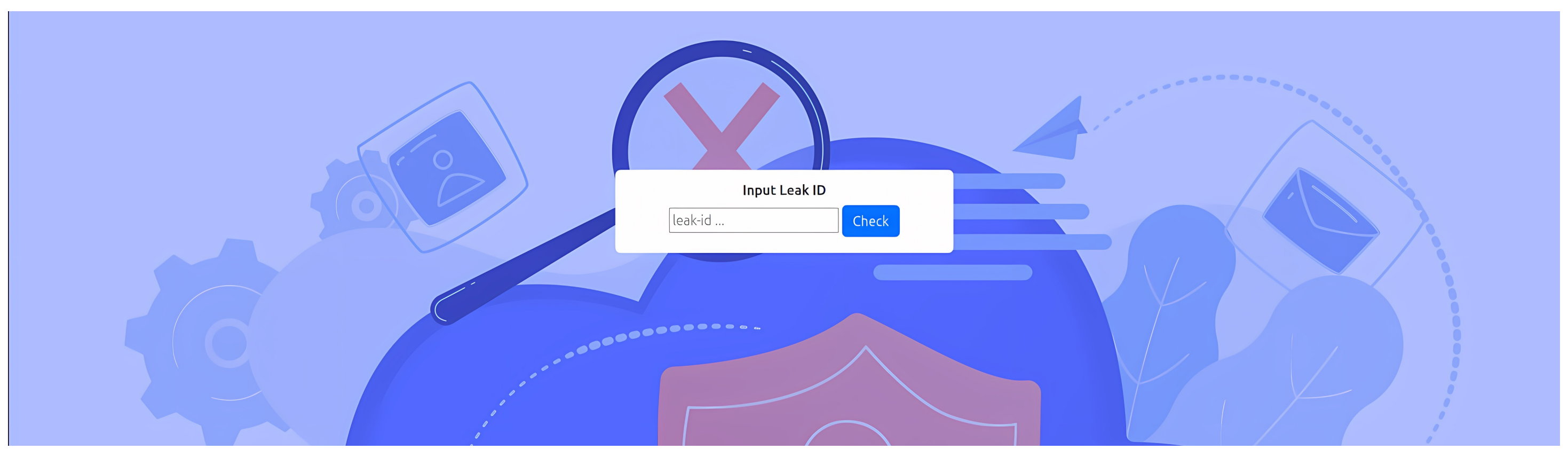
At the same time, IT-security requirements and data privacy requirement have to be adhered to. To overcome these challenges, a variety of concepts for taking in data from companies or users to check were analysed. The analysis focused on ensuring that they can both guarantee protection of whistleblowers as well as enable the requirements of the processing and analysis mechanism.

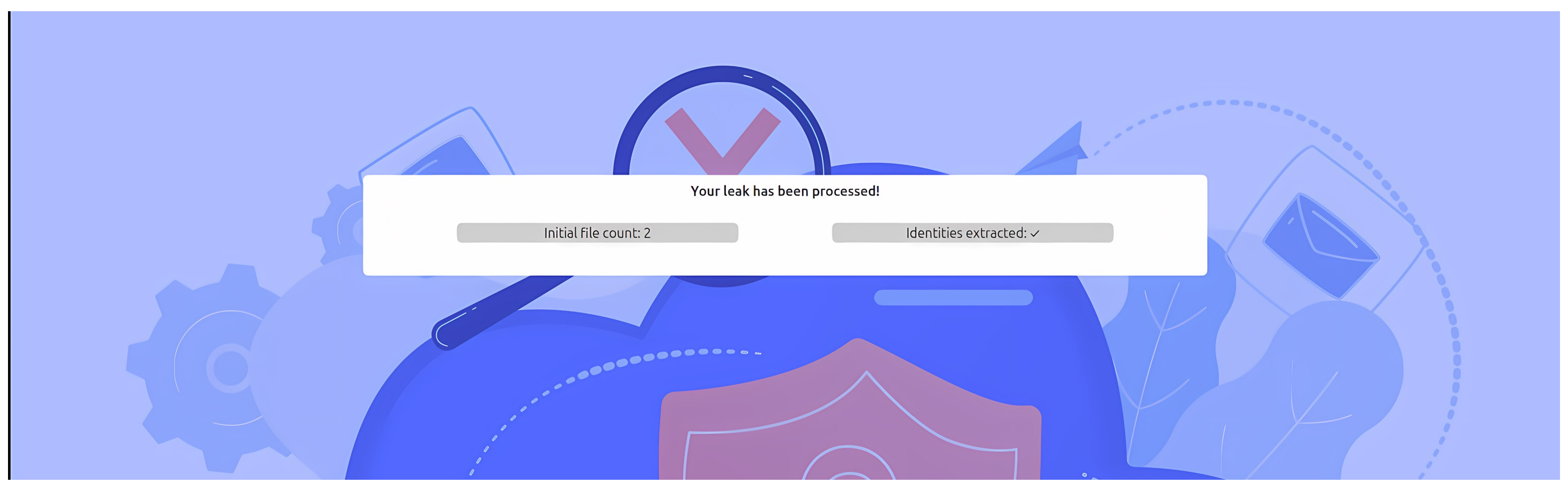
Identities and Partial Identities

- How do we define identities, and when is an identity identifiably unique?
- => No legal definition, thus defined based on technical requirements

Which incentives do we want to set for data delivery?

- (Anonymous) Information about processing and usage




Your leak has been processed!

Initial file count: 2

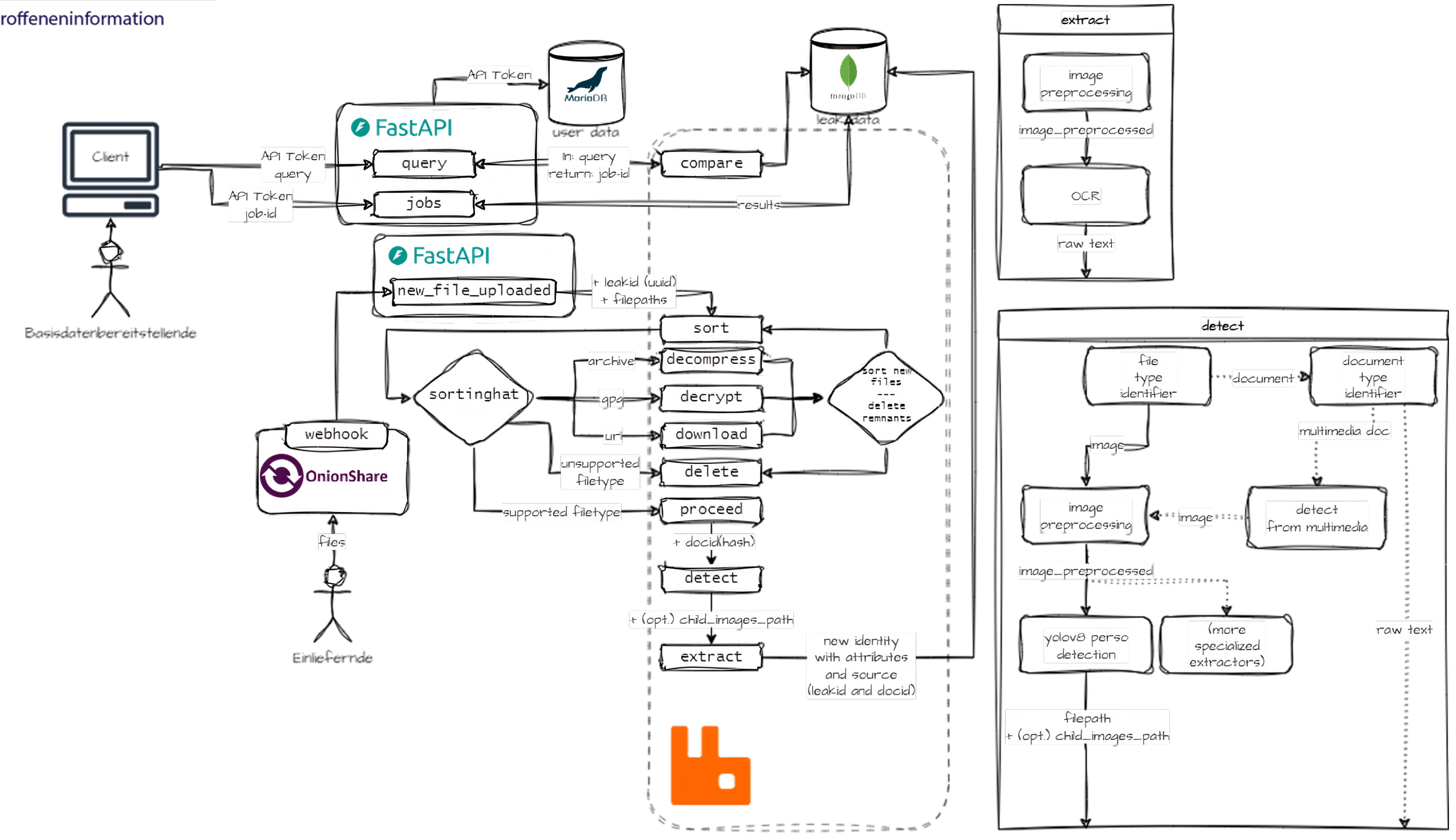
Identities extracted: ✓

Components

- Dropzone (Ingestion) (AP 2)
  - Upload over HTTPS or TOR (Onionshare)
  - Pre-processing (e.g. ID Card recognition, OCR)
  - Log and save as little as possible
- Data Cleaning (AP 3)
  - Discarding data that is not used
- (AP 3)
  - Mechanism to check existing clear text data with stored anonymous data
- Warning messages (AP 4)
  - Concept to generate warnings

Use Cases

- External service for companies or institutions
- Deployment directly at internal or external whistleblowing reporting offices according to HinSchG (Hinweisschutzgesetz)



Legal Aspects:

Lawfulness (Art. 5 (1) a GDPR) – no usage when obviously unlawful. But: The objective is to warn about data leaks, so it is about data that is already lost. The goal is to give some control back to data leak victims, in accordance with the objectives of the GDPR. Minimal data retention, no readable data, only hashes.

Legal Basis for processing – Art. 6 Abs 1 f GDPR, legitimate interest. Objective is the protection of privacy. It is required as there is no other, lesser means in case of an existing data leak. Data is usually already in circulation. (Consideration of protection of imapcted data subjects interests vs human rights and constitutional freedoms) Protection of data subjects rights of primary importance, but also a very high interest in warning data subject and possible prevention of follow-on damages. => legitimate interest in processing, processing made less harmful through special TOM (Technical and organisational means)

Storage obligations – No storage obligations pursuant to TKG, TDDDG, DDG, DSA. Possible data requests by law enforcement agencies. If there is a request, check for plausibility, ensure as little data as possible is available.

Possible Criminal Mögliche Strafbarkeit – No criminal liability pursuant to § 202a StGB, § 42 (1) Nr. 1 and 2 and (2) Nr. 1 BDSG or § 202d StGB. Also no violation of business secrets or copyright law. However, open questions remain in case of consideration of rights and edge cases.

Prof. Dr. Franziska Boehm (KIT) – franziska.boehm@kit.edu
Prof. Dr. Michael Meier (UBO) – mm@cs.uni-bonn.de
Project Coordinators
https://itsec.cs.uni-bonn.de/drops/
2023-2025 Karlsruhe, Bonn

Funded by
the European Union

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung