UNIVERSITÄT
LEIPZIG

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

# RAKI – Rapide Erklärbare KI

## Konzeption und Umsetzung von Datenschutz- und Privacy-Mechanismen

**René Speck**[1] *rene.speck@uni-leipzig.de*

[1]Universitätsrechenzentrum, Universität Leipzig

(Projektnummer: 32100687, Förderkennzeichen: 01MD19012D)

# Inhalt



**Warum?**

- Schutz der Menschen
- Schutz vor Auswirkungen auf Menschen
- Wahrung des Persönlichkeitsrechts
- Recht auf Informationelle Selbstbestimmung

**Wie?**

- Rechtmäßig und Transparent
- Datensparsamkeit und Speicherbegrenzung
- Zweckbindung
- Richtigkeit
- Rechenschaftspflicht

**Beim Design beachten:**

- Stand der Technik
- Kosten
- Verarbeitungsart, -umfang , -kontext,-zweck
- Risiken

**Personenbezogene Daten:**

- IP-Adressen
- E-Mail Adressen
- Telefonnummern
- Kundennummern

# Datenschutzrisiken

**Risiken:**

- IP Adressen
- Benutzernamen etc. in Trainingsdaten
- Anlagendaten mit personenbezogenen Daten
- Experten im Lernprozess
- Expertenfeedback

**Verarbeitungsart, -umfang , -kontext,-zweck:**

- Speicherung in Datenbanken auf lokalem Server
- Nachdem die Konfigurationen gelernt wurden, können Daten (Trainingsdaten) gelöscht werden.
- Das Expertenfeedback kann nach Verarbeitung gelöscht werden

Alle Forschungsarbeiten werden nach dem **FAIR-Datenprinzip** durchgeführt:

Data and supplementary materials have sufficiently rich metadata and a unique and persistent identifier.

**FINDABLE**

Metadata and data are understandable to humans and machines. Data is deposited in a trusted repository.

**ACCESSIBLE**

Metadata use a formal, accessible, shared, and broadly applicable language for knowledge representation.

**INTEROPERABLE**

Data and collections have a clear usage licenses and provide accurate information on provenance.

**REUSABLE**

**Datensätze:**

- Konfigurationen
- Trainingsdaten
- Anlagedaten
- Expertenfeedback


GDPR-konforme Datenschutzerklärung:

- `https://gdpr.eu/privacy-notice/`
- `https://gdpr.eu/wp-content/uploads/2019/01/Data-Processing-Agreement-Template.pdf`

# Anwendungsfälle: AI4BD und Siemens AG

Kundennamen `customer_name` in den Datensätzen müssen anonymisiert werden ebenso Kundennummern `customer_number` und ggf. -ids `customer_id`.

Ein Kunde könnte anhand von speziellen Bauelementen, die nur dieser Kunde oder in dieser Kombination in der Produktlinie bestellt, identifiziert werden.

# Anonymisierung

- Directory Replacement
  - `customer_name`
  - `customer_number`
- Masking
  - `customer_number`
- Scrambling
  - `customer_id`
- K-Anonymization

**Horizon 2020-Projekt SPECIAL**: Skalierbare richtlinienorientierte auf Linked Data basierte Architektur für Datenschutz, Transparenz und Regelüberwachung.

**Vokabulare**:

- **spl**: The SPECIAL Usage Policy Language
- **splog**: The SPECIAL Policy Log Vocabulary

**Berechtigungen** (`spl:Authorization`):

**Abstrakte Nutzungsrichtlinie (5-Tupel)**

```
<data item, purpose, operation, storage, recipient>
```

jede eine zulässige Operation

**Beispiel, Nutzungsrichtlinie P**

```
<feedback.jsonld, Feedback, Analyze, OurServers, SIEMENS>
```

Ermöglicht es dem Unternehmen SIEMENS die Datei feedback.jsonld auf lokalem Server für Feedback zu analysieren, wenn eine entsprechende Berechtigung zu P gehört.

# The SPECIAL Usage Policy Language (spl)

Nutzungsrichtlinie besteht aus mindesten einem OWL 2 Ausdruck.

```
ObjectUnionOf(
    ObjectIntersectionOf(
        ObjectSomeValuesFrom(spl:hasData PersonalData)
        ObjectSomeValuesFrom(spl:hasProcessing spl:AnyProcessing)
        ObjectSomeValuesFrom(spl:hasPurpose NonCommercial)
        ObjectSomeValuesFrom(spl:hasRecipient spl:Null)
        ObjectSomeValuesFrom(spl:hasStorage spl:Null)
        )

    ObjectIntersectionOf(
        ObjectSomeValuesFrom(spl:hasData PseudonymizedData)
        ObjectSomeValuesFrom(spl:hasProcessing spl:AnyProcessing)
        ObjectSomeValuesFrom(spl:hasPurpose spl:AnyPurpose)
        ObjectSomeValuesFrom(spl:hasRecipient spl:AnyRecipient)
        ObjectSomeValuesFrom(spl:hasStorage spl:AnyStorage)
        )
)
```

Eine allgemeine Nutzungsrichtlinie: *ObjectUnionOf*(*BasicPolicy*$_1$ . . . *BasicPolicy*$_n$)

# The SPECIAL Usage Policy Language (SPL)

```
ObjectIntersectionOf(
    ObjectSomeValuesFrom(spl:hasData SomeDataCategory)
    ObjectSomeValuesFrom(spl:hasProcessing SomeProcessing)
    ObjectSomeValuesFrom(spl:hasPurpose SomePurpose)
    ObjectSomeValuesFrom(spl:hasRecipient SomeRecipient)
    ObjectSomeValuesFrom(spl:hasStorage SomeStorage)
)
```

- SomeDataCategory: `svd:Anonymized`, `svd:Statistical`, ...
- SomeProcessing: `svpr:Anonymize`, `svpr:Collect`, ...
- SomePurpose: `svpu:Feedback`, `vpu:Login`, `svpu:Develop`,
- SomeRecipient `svr:Delivery`, `svr:Ours`, `svr:Public`,, ...

# Storage Expressions

```
ObjectIntersectionOf(
    ObjectSomeValuesFrom(spl:hasLocation SomeLocation)
    ObjectSomeValuesFrom(spl:hasDuration SomeDuration)
    DataSomeValuesFrom(spl:durationInDays Interval)
)
```

- SomeStorage `svl:OurServers`, `svl:ThirdParty`, `svdu:StatedPurpose`, `svdu:Indefinitely`, ..

# The SPECIAL Policy Log Vocabular (splog)

Verwendete Vokabulare:

- The SPECIAL Usage Policy Language für Datenschutzrichtlinien
- Provenance Ontology für Provenienz Informationen
- Dublin Core Terms für Metainformationen

Log Inhalt ist von der Klasse `splog:LogEntryContent` einer `rdfs:subClassOf` der `spl:Authorization`.

Auf diese Weise können Berechtigungen für Ereignisinhalte und Datenrichtlinien auf Konformität überprüft werden.

# Beispiel Sensordaten

```
befit:entry3918  a splog:ProcessingEvent;
  splog:dataSubject  befit:Sue;
  dct:description  "Store location in our data base in Europe"@en;
  splog:transactionTime  "2018-01-10T13:2050Z"^^xsd:dateTimeStamp;
  splog:validityTime  "2018-01-10T13:20:00Z"^^xsd:dateTimeStamp;
  splog:eventContent  befit:content3918;
  splog:inmutableRecord  befit:iRec3918.

befit:content3918  a  splog:LogEntryContent;
  spl:hasData  svd:Location;
  spl:hasProcessing  befit:SensorGathering;
  spl:hasPurpose  befit:HealthTracking;
  spl:hasStorage  [spl:haslocation svl:OurServers];
  spl:hasRecipient  [a svr:Ours].
```

Im Projekt für Expertenfeedback, Anlagedaten, Sensordaten, ...

# Vielen Dank

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

UNIVERSITÄT
LEIPZIG

René Speck
Universität Leipzig
Universitätsrechenzentrum
Augustusplatz 10
04109 Leipzig

rene.speck@uni-leipzig.de
www.urz.uni-leipzig.de