Proposal of decentralized police database system

- **EU Commission activities**
  - Commission realises industry's problem (COM(2012) 417)
  - Solution: Privacy by Design in addition to regulation
  - New data protection rules (COM(2012) 11) provide for PbD standards

- **Proposal of decentralized police database system from a legal perspective using the example of Germany and the EU**

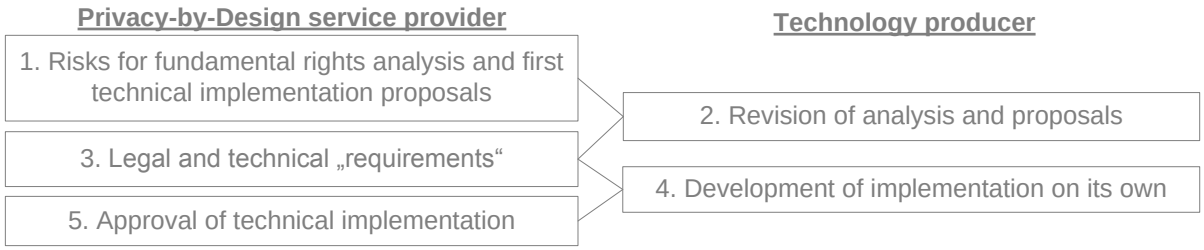
- **Idea from integration research project funded by** Federal Ministry of Education and Research

- Digi-Dak **Digital contact-less fingerprint-trace capture**

- **Structure: 15 mins presentation and discussion**

Contact-less fingerprint acquisition & Privacy-by-Design method

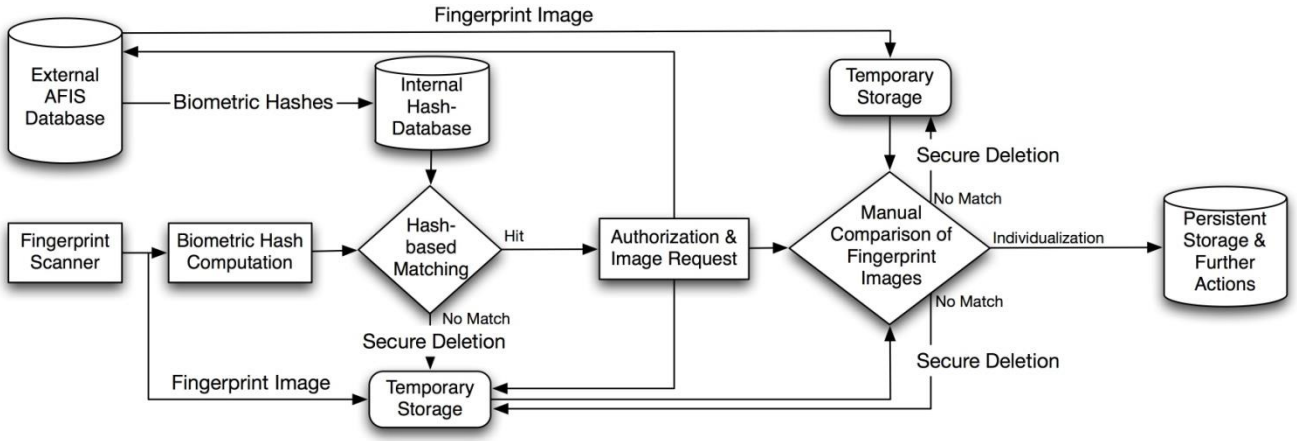
-   **New use-cases, risks and possible solution**
- **State of the art and legal requirements**
- **Basic properties of the Privacy-by-Design method**
  - Bridging-approach for close cooperation of lawyers & engineers



  - Justify design decisions using legal arguments
  - Distinguishing general requirements from specific implementation
  - Goals : pseudoidentifiers, decentralisation, graded data capture
  - Comprehensive assessment

General technical design approach

- **Design approach**



- **Integration into overall system**
  - Coarse scan & aging
  - "Two-offices principle"
  - Manual error management (ACE-V)
- **Distinguishing general approach from specific implementation**
  - Correct balance of citizens' and producers' freedoms
  - Requirement vs. example of compliance

Specific technical implementation

- **Multiple 1-to-1 verifications based on biometric hashes**
- **Database**
  - Table "reference_data": biometric hashes & keys for AFIS
  - Table "capture_data": hashes of scanned FPs, meta-data & reference
- **Temporary storage of FP images, individual encryption & deletion**
- **Biometric hash based matching**
- **An examiner is alerted if a positive match is found**
  - Image requested from AFIS
  - Access granted for the expert
  - If no match: images securely deleted
  - If match: time & date transferred to a persistent storage

Benchmark using legal arguments

- Transparency
- System suitability
- Use limitation
- Data security
- "System protection"
- Data minimisation
- Accountability
- Uniform Identifiers
- False hits
- Sensitive data
- Distinction non-/suspects & facts/assumptions
- "High Scatter"
- Instant erasure
- Indiscriminate data collection

Conclusions and future work

- **Conclusions**
  - Legally preferable to take a decentralized database approach
  - Technical and legal analysis of specific implementation
  - Integration helps assess overall privacy impact
  - Distinguishing general requirements from specific impl'
- **Future work**
  - Performance of biometric hashes in forensics
  - Reconstruction of biometrics and collisions of hashes
  - Rules for privacy protecting concepts used by industry for public acceptance
- **Discussion …**