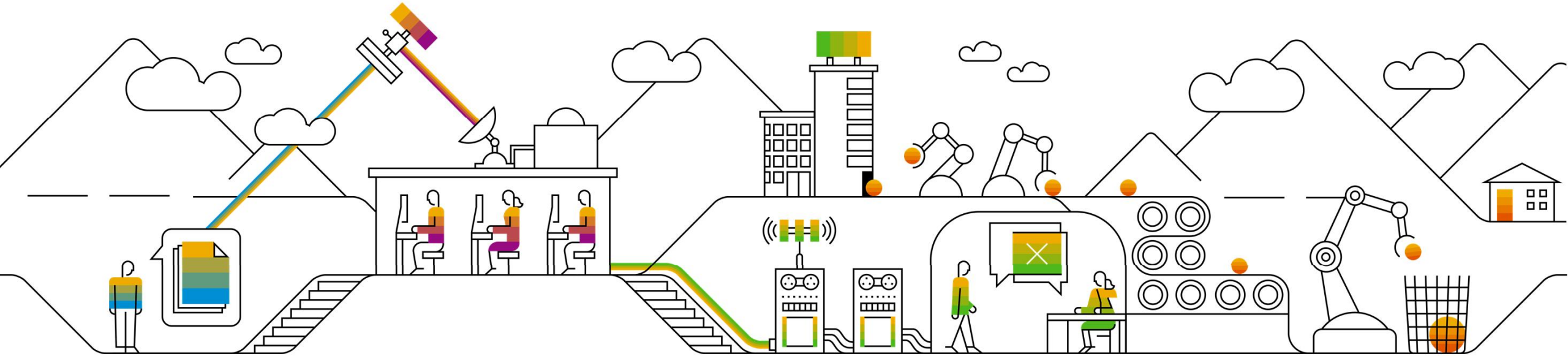


Procedure model for a GDPR project in SAP Business Suite / S/4 HANA

Ksenia Tretjakova (SAP Deutschland SE)

CUSTOMER

SAP Run Simple

SBNNORGE

Disclaimer

SAP does not provide legal advice, nor does the presenter.

The implementation of data protection requirements at any data controller is a complex challenge with interdependent legal and technical aspects. The responsibility to identify and implement adequate technical features remains with the controller as for the organizational aspects.

The following presentation is only about technical features which might in that sense help a controller achieving compliance with data protection regulations.

To help the audience understanding the shown approach, in context information is given without claiming completeness or correctness.

Implementation approaches

Deductive approach

- Description of the processing purposes and processing operations
- Regardless of the technical approach and real data set

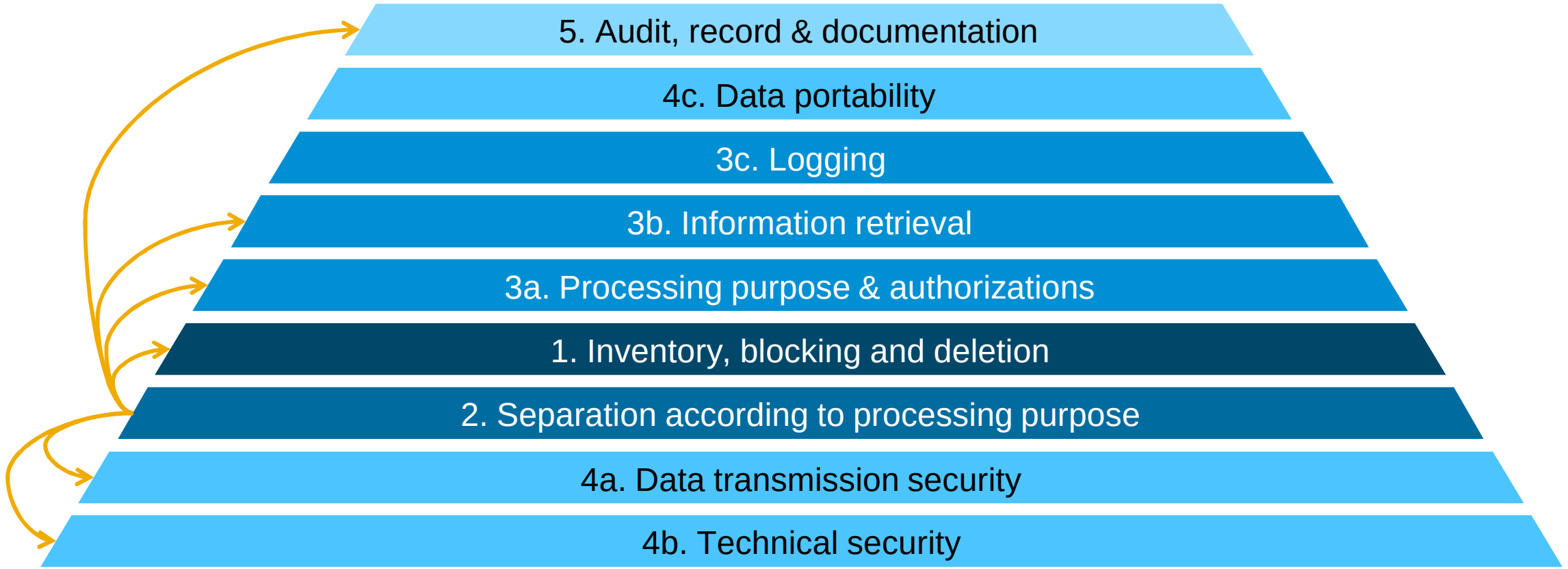
Inductive approach

- Identification of the personal data located in the relevant systems
- Technical transparency regarding personal data
  - Regardless of systemic boundaries, processing purposes and controller
  - Inventory and scoping

Our recommendation:

Deductive approach for new systems, inductive approach for existing systems

Procedure model for the inductive approach



Source: Rheinwerk Verlag: Lehnert, V. et.al.; *Datenschutz in SAP Business Suite und S/4HANA*; publication date 12 2017.

Procedure model for the inductive approach

Step 1: Inventory, blocking and deletion

Identification of personal data, for

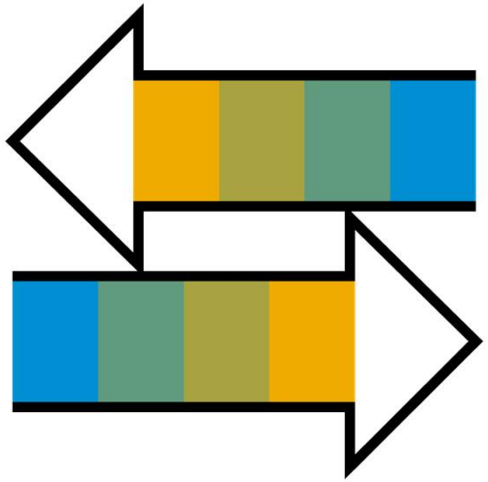
- Blocking and deletion
- Information retrieval
- Record of processing activities

As part of the blocking and deletion the following information is gathered

- Data structures and dependencies between data
- Data inconsistencies
- Organizational structures
- Missing technical attributes for defining the processing purpose

Procedure model for the inductive approach

Step 2: Separation According to processing purpose



Documentation of the processing purpose, for

- Blocking and deletion
- Authorization concept
- Record of processing activities
- Information retrieval

Review of definitions for

- Organizational structures – line-organizational attributes (LOA)
  – Explicit definition of the controller
- Master data structures – process-organizational attributes (POA)
  – Explicit depiction of the processing purpose

Procedure model for the inductive approach

Step 3a: Processing Purpose & Authorizations

Projection of processing purpose through authorizations, via

- Organizational differentiation – line-organizational attributes (LOA)
  – Access to personal data restricted to the processing of one controller
- Differentiation of processing purpose – process-organizational attributes (POA)
  – Access to personal data restricted to the processing purpose

Implementation of permitted activities

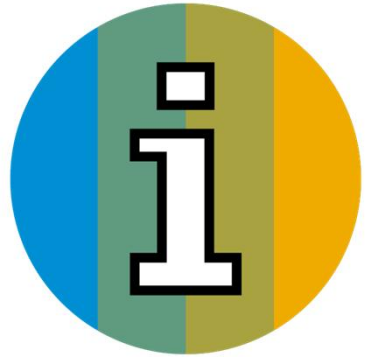
- Functional specification of access authorizations
- Strictly implemented minimum principle also for read-only authorizations
- Definition of access risks in relation to LOA and POA

Procedure model for the inductive approach

Step 3b: Information retrieval

Re-use of the identified personal data

- Identified ILM-objects as base
  - ILM objects containing personal data are the base for Information retrieval
- Retention Rule Generator provides the processing purpose
  - Interlinkage between the ILM-object and the purpose of processing



Categorizing the Information retrieval model, for:

- Information – to be provided
- Information Retrieval Framework
- Record of processing activities

Procedure model for the inductive approach

Step 3c: Logging

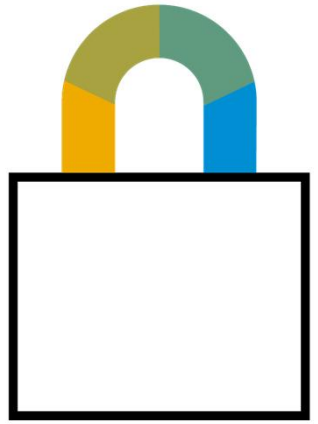
Ensuring the necessary logging functionalities, via

- Control configuration for logging, such as:
  - System-log
  - Transport logging
  - Table logging – particularly for custom configurations
  - Security Audit Log
  - Change log – particularly for custom functions
- **Read Access Logging or UI-Logging**
  - Logging of read access especially to sensitive personal data
  - SAP template configuration is set in consideration of sensitive personal data (Art. 9, par. 1 EU GDPR)

Procedure model for the inductive approach

Step 4a: Data transmission security

Safeguarding the data transmission, via



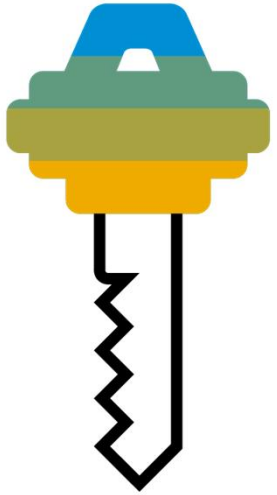
- Record of possible and used interfaces
  - Using the interface landscape identified during the data blocking and deletion phase as a basis
- Identification of the processing purpose for the interfaces
- Transmission restriction according to the processing purpose
  - Appropriately defined authorizations for system users within the RFC connections
  - Using UCON to restrict function modules that can be called by RFC
- Data transfer encryption
  - Particularly for external recipients
  - Communication safeguarding (e.g. RFC, Client/Server)

Procedure model for the inductive approach

Step 4b: Technical Security

In addition to the already presented measures

- Authentication control
  - Secure procedures to enable system access based on personal authentication
- Access control – prevent security vulnerabilities
  - Import of security notes
  - Screen for security vulnerabilities in custom code
- Availability control
  - Data backup & recovery
  - Business continuity
- Configuration settings controls
  - SAP Configuration Validation
  - SAP Early Watch Alert
  - SAP Security Optimization Service

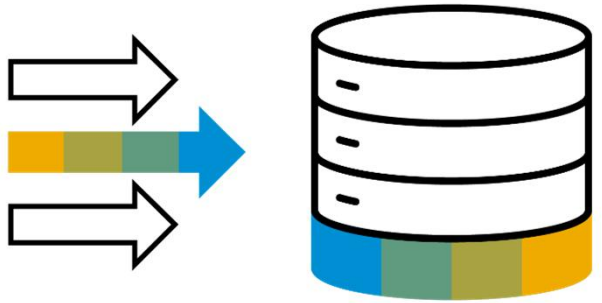


Procedure model for the inductive approach

Step 4c: Data Portability

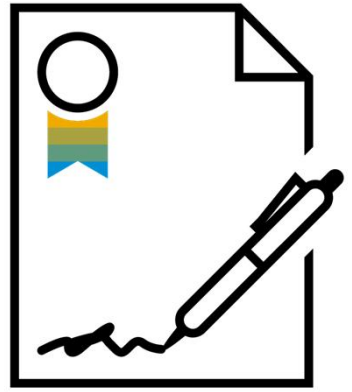
Information retrieval based on:

- Data identified during the information retrieval phase
  - Provide personal data in a structured, commonly used and machine-readable format
  - Information Retrieval Framework



Procedure model for the inductive approach

Step 5: Audit, record & documentation



Record obligations

- Record of processing activities
- Record of technical and organizational measures
- Record of control (ICS)

Obligatory content:

- Documentation of the processing purpose and retention periods via LOA and POA
- Documentation of record to ensure correctness of personal data
- Documentation of record to ensure restricted access
- Documentation of Information retrieval and information process
- Documentation of interfaces
- Documentation of security safeguards

Thank You

Ksenia Tretjakova
Technical Security Consultant
Practice Unit DTS GRC / Security

SAP Deutschland SE & Co. KG

T +49 61 421891015 **M** +49 151 43819732
k.tretjakova@sap.com

Run Simple

Follow us

www.sap.com/contactsap

THE BEST RUN SAP®