Purposes of the processing
Basis for any processing

PUBLIC

SAP Run Simple

Disclaimer

SAP does not provide legal advice nor does the presenter.

The presenter is not a lawyer.

The following presentation is only about technical features which might help a customer to become compliant with data protection regulations.
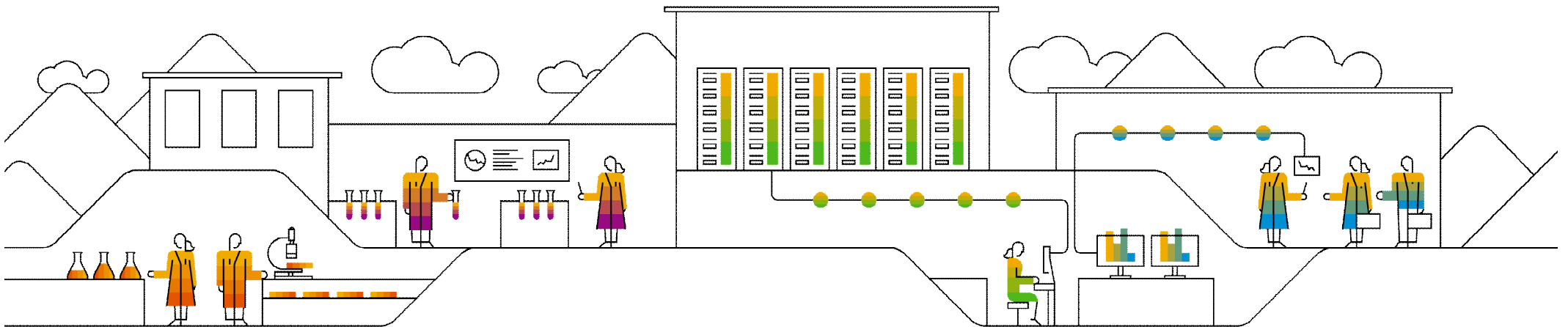
To help the audience understanding the approach and the need, some context information is given without claiming completeness or correctness.
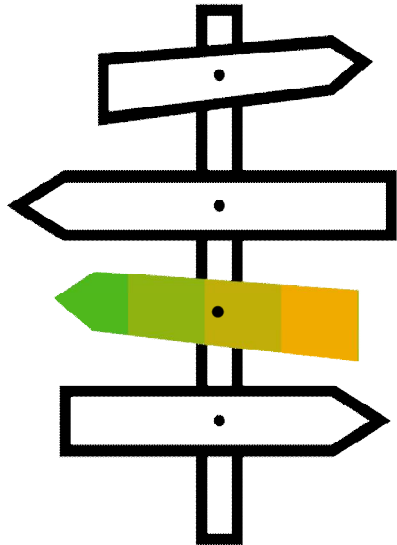
Agenda

Purpose & Processing

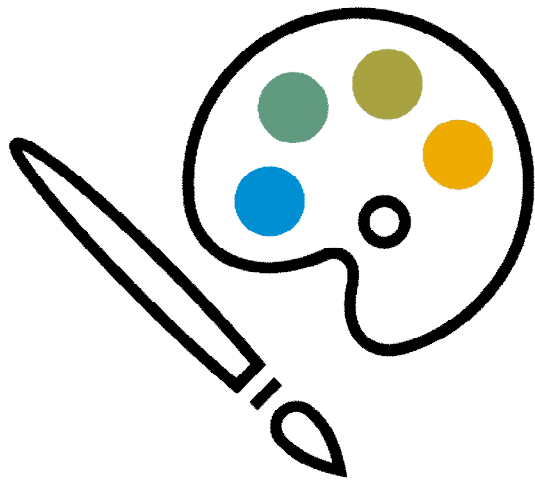Separation by Purpose

Purpose & Processing

Processing of Personal Data Based on Purposes

Any processing of personal data is based on a "*specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". (Art. 5 Par. 1 Lit. b EU GDPR)

My purpose is …

Purpose in GDPR terms

is not about your **ideas what you could do** with personal data

is not about **generic marketing slogans** even if they are part of a companies mission

is absolutely nothing what you are not able to **specifiy explicitly** when the processing starts
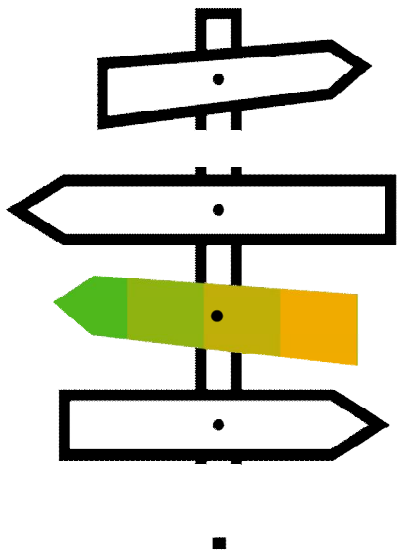
is in any case based on the **legal reasons** to process personal data defined in **Art. 6 (1) GDPR**.

Processing of Personal Data
Legal Basis
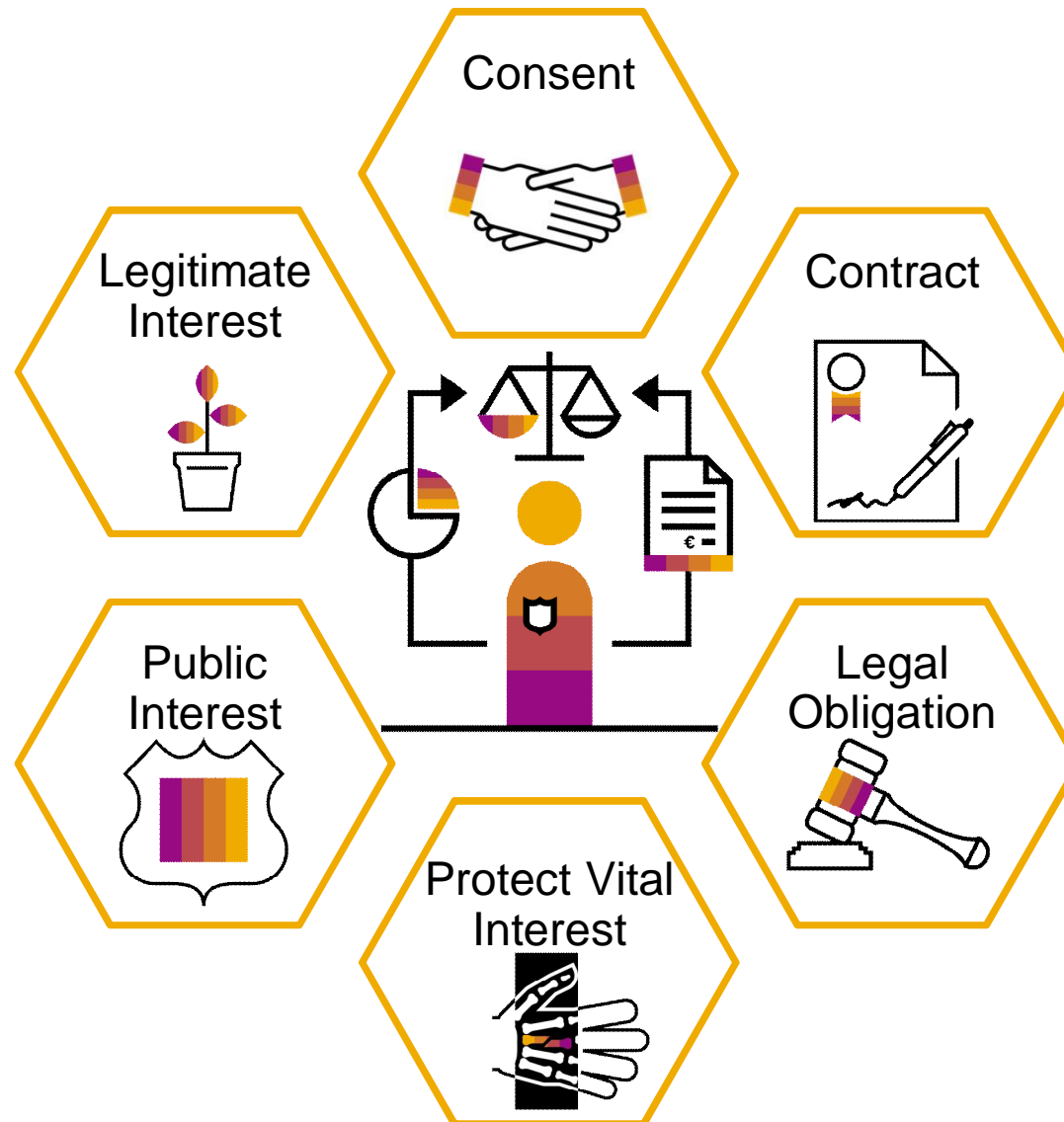
Processing of Personal Data Based on Purposes

Any processing of personal data is based on a "*specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". (Art. 5 Par. 1 Lit. b EU GDPR)
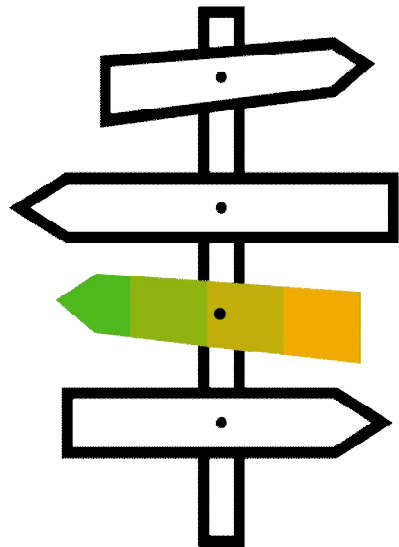
Processing is **legitimated** by:
Consent **or** contract **or** legal obligation **or** the protection of vital interest **or** public interest **or** a legitimate interest of the controller. (Art 6. Par. 1 EU GDPR).

The term **purpose** itself is not defined. Different models are possible.

Processing of Personal Data Based on Purposes

Any processing of personal data is based on a "*specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". (Art. 5 Par. 1 Lit. b EU GDPR)

Processing is legitimated by:
Consent or contract or legal obligation or to protect vital interest or in public interest or by a legitimate interest of the controller. (Art 6. Par. 1 EU GDPR).

The term **purpose** itself has to be interpreted by our customers. However, the following applies:

- There is a logical link to the relevant business processes

- Attributes are required to mark data as related to a certain purpose

- The amount of defined purposes has an increasing impact on the measures to be taken in the system

Processing of Personal Data Based on Purposes

Any processing of personal data is based on "*specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". (Art. 5 Sec. 1 Lit. b EU GDPR)

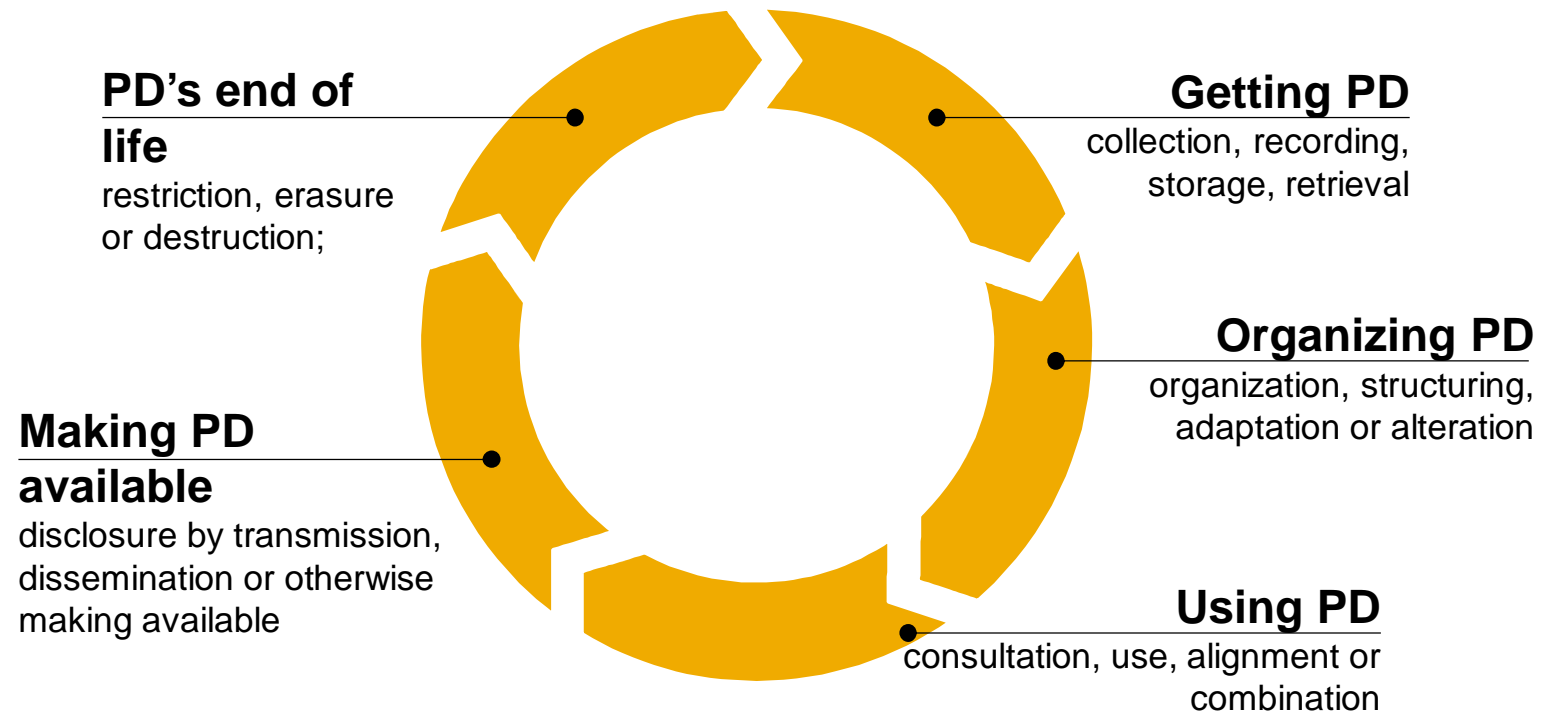Processing is simply <u>any</u> operation on personal data. (Art. 4 Sec. 2 EU GDPR)

The purpose is defined by the controller or joint controllers. (Art. 4 Sec. 7, Art. 26 EU GDPR)
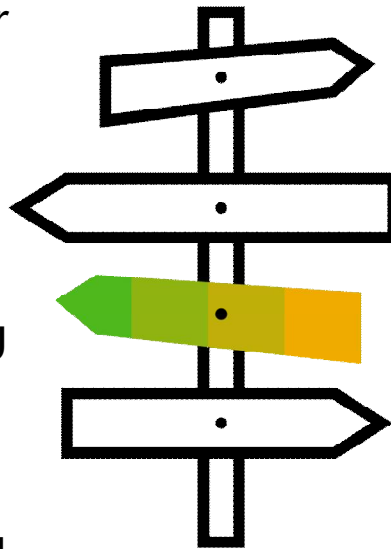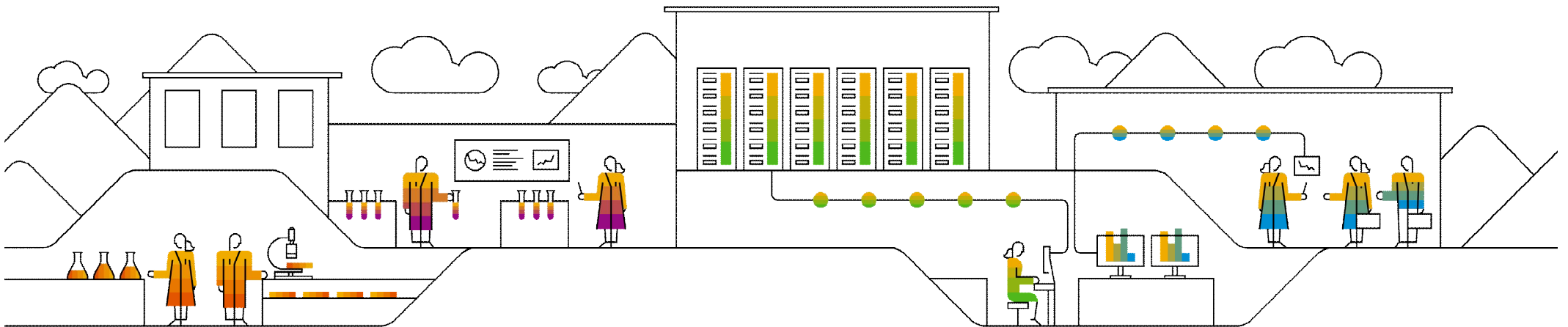
A controller is a "*natural or legal person, public authority, agency or other body*". (Art. 4 Sec. 7, EU GDPR)

For any operation, you need to prove that this operation is based on the specified purpose. Any purpose is linked to at least one controller.

Processing of Personal Data in the Lifecycle

PD's end of life
restriction, erasure or destruction;

Getting PD
collection, recording, storage, retrieval

Organizing PD
organization, structuring, adaptation or alteration

Making PD available
disclosure by transmission, dissemination or otherwise making available

Using PD
consultation, use, alignment or combination

Separation by Purpose

Separation by Purpose
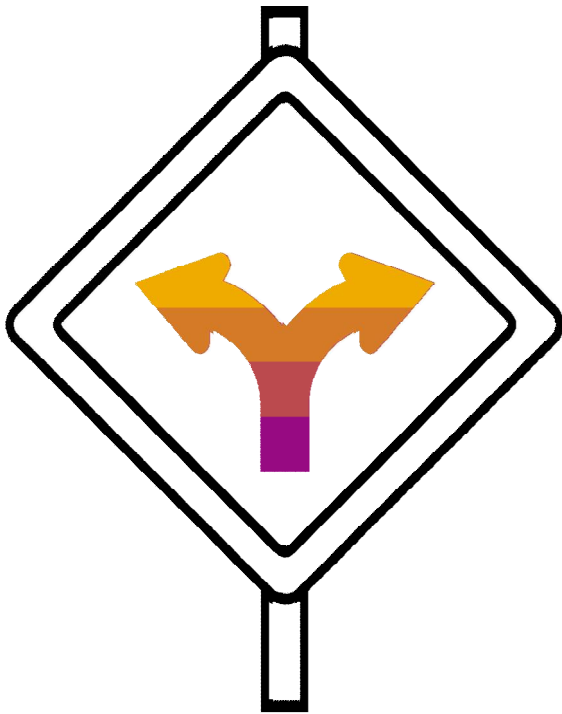
The easiest way to separate by purpose is to have one tenant per purpose. Obviously, this will cause heavy costs of ownership. So, in what other way can separation by purpose be done? We assume there are two options:

- Relating data to an attribute "purpose"
- Relating data to line organizational attributes (LOA) and process organizational attributes (POA)

The second option is the preferred one, because these attributes are – among many other reasons – also relevant in terms of other business legislation, such as financial legislation. Apart from that, these attributes are already given in existing products.

But How to Separate?
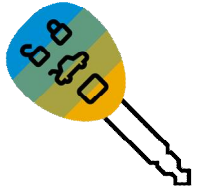
Any kind of access must be controlled by authorizations according to the purpose. This includes access by persons, machines, software logic and any kind of transmission. For this reason, the data needs attributes reflecting:

- the purpose or
- line organizational and process organizational attributes

Once the primary purpose has ended, personal data must either be deleted or – in case of other applicable retention periods – the data must be blocked. For this reason, data again needs attributes reflecting

- the purpose or
- line organizational and process organizational attributes

Any data subject has the right to request information on all his/ her data undergoing processing. This information must be structured by purpose and must be given along with the information which retention periods apply. So again, the data needs attributes reflecting

- the purpose or
- line organizational and process organizational attributes

Long story short: most additional data protection requirements need these attributes.

What Does "Line Organization" Mean?
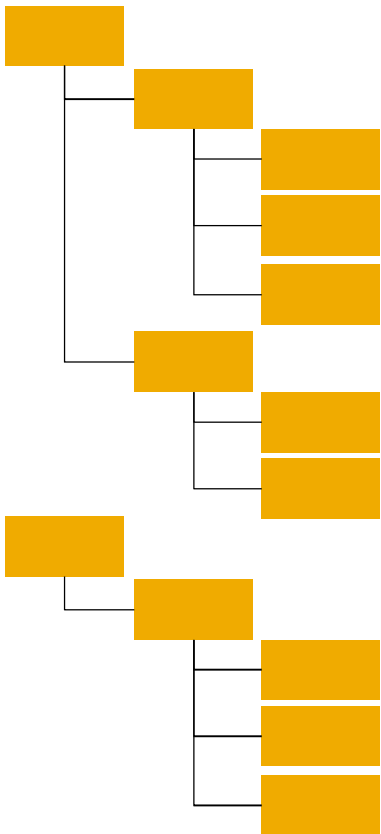
The term "line organization" is taken from business administration science. Every organization has a formal hierarchical structure. In business administration, the term "controller" describes the independent accounting unit or the legal entity.

To make it explicit: None of us has a contract with SAP. SAP is not a legal entity, but a "group of companies". The presenter has a contract with SAP SE, some consultants with SAP Deutschland SE & Co. KG, some of us with SAP America, Inc.

In SAP Business Suite and SAP S/4HANA, the legal entity is in most cases reflected by the company code as the „independent accounting unit".

What Does "Process Organization" Mean?

The process organization reflects the sum and interdependencies of all business processes running in an organization.

A business process is a targeted, temporally logical, self-contained sequence of tasks that can be executed by several organizational units or organizations to distribute the work.
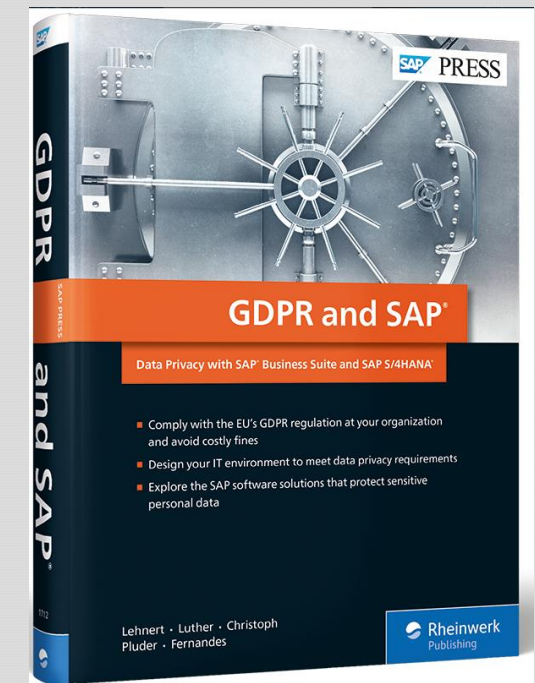
Purpose of the Data Undergoing Processing
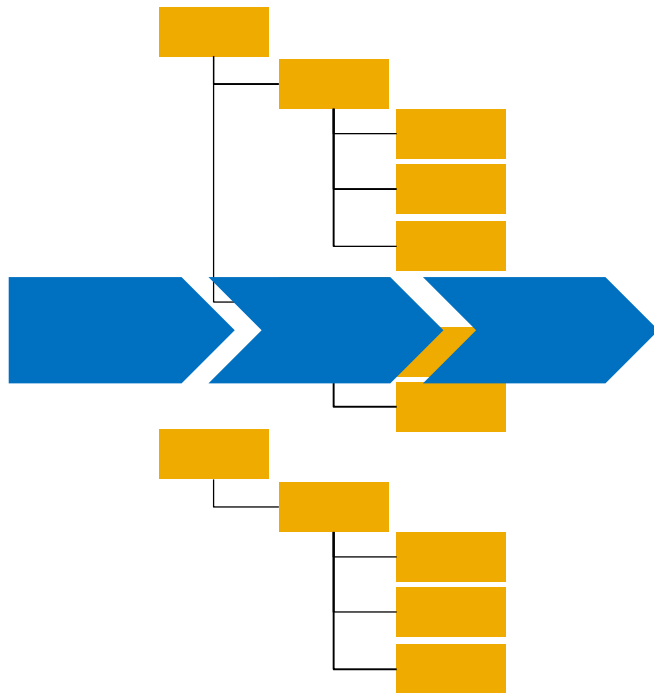
The purpose of the data undergoing processing is inherently defined by a combination of legal entity and the business process in which the data is used.

Parts of the presentation are taken from "Datenschutz mit SAP, Lehnert et. al. 2017, available soon in English "GDPR and SAP"

Thank you.

Contact information:

Volker Lehnert
Senior Director Data Protection & Privacy
S/4HANA