Bud P. Bruegger, ULD, "Verfahrensmodell – Model of Data Processing", Folien zur internen Diskussion, Version 16. April 2018.

Download URL:
https://www.datenschutzzentrum.de/uploads/projekte/ikopa/ModelOfProcessing-V16_5_2018.pdf

Nachstehender Foliensatz des Modells wurde im April 2018 ULD-intern diskutiert. Das konzeptionelle Verständnis des Verarbeitungsbegriffs und die Entwicklung des Modells war Teil der Forschungstätigkeit im Rahmen der vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts iKoPA [1].

[1] https://www.datenschutzzentrum.de/projekte/ikopa/ , https://ikopa.de/

iKoPA

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

ULD Montagsdiskussion nach Lage

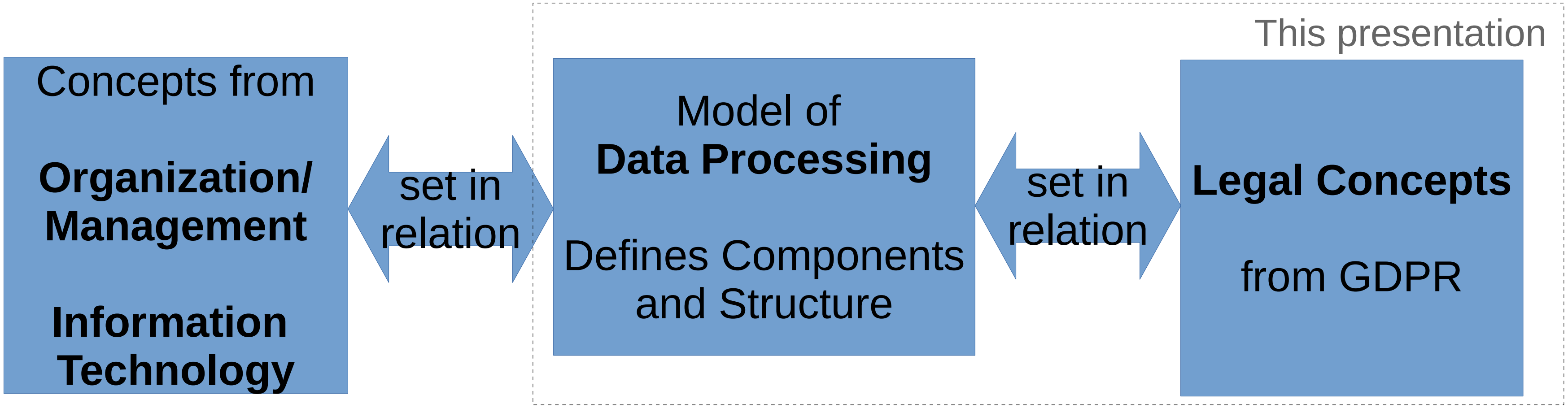
Verfahrensmodell
–
Model of Data Processing

Bud P. Bruegger

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Objectives

- Provide a **More Precise Language**
  - specific component/aspect instead of just "data processing"
  - well-defined relations between concepts (ontology)
- **Create a Common Understanding** of Concepts between
  - Lawyers
  - IT and Management Professionals



Approach

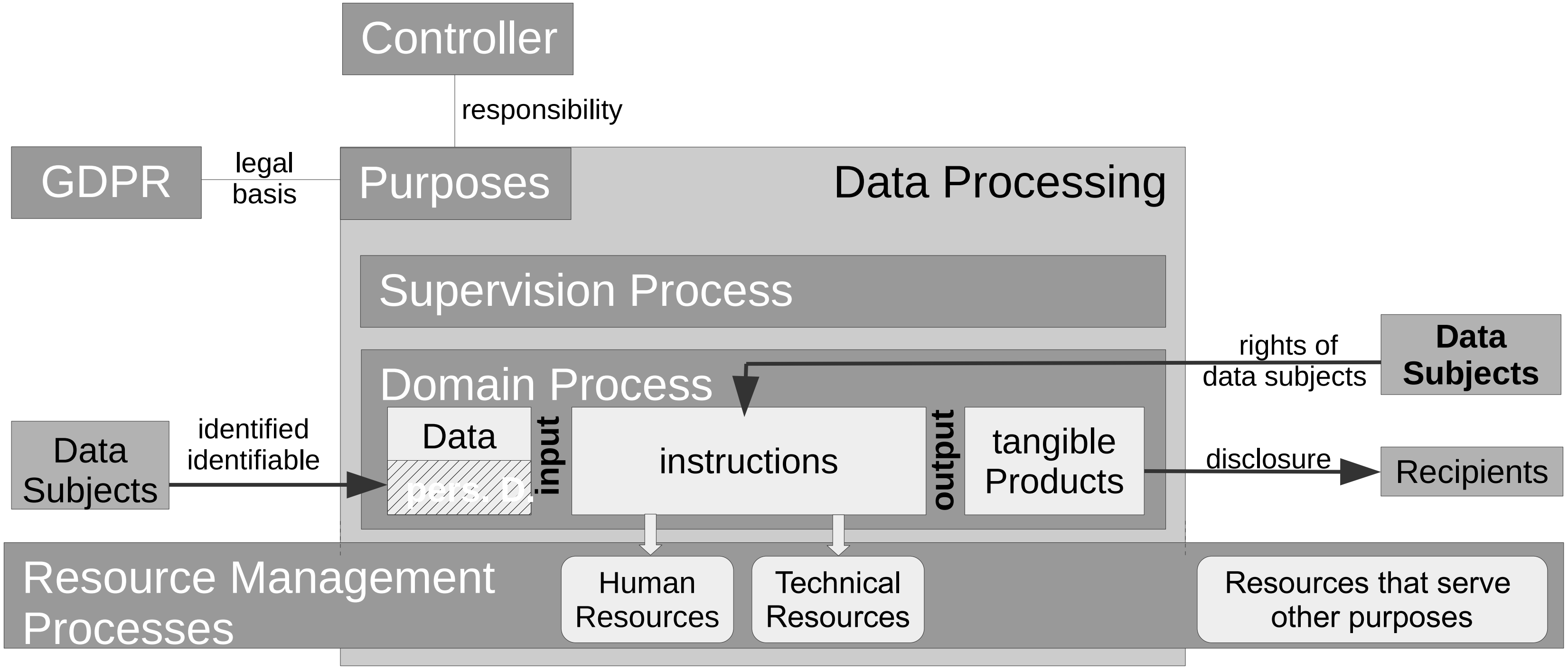
- GDPR (in English, German version is semantically different!)
  - Natural Language Analysis
    - term extraction:
      - what are the terms used to describe „data processing“?
    - extraction of relations:
      - what relations between these terms are expressed?

- Map these terms graphically in a Figure (the Model of DP)
  - Use IT concepts to help structure/complete the Figure

Some Applications

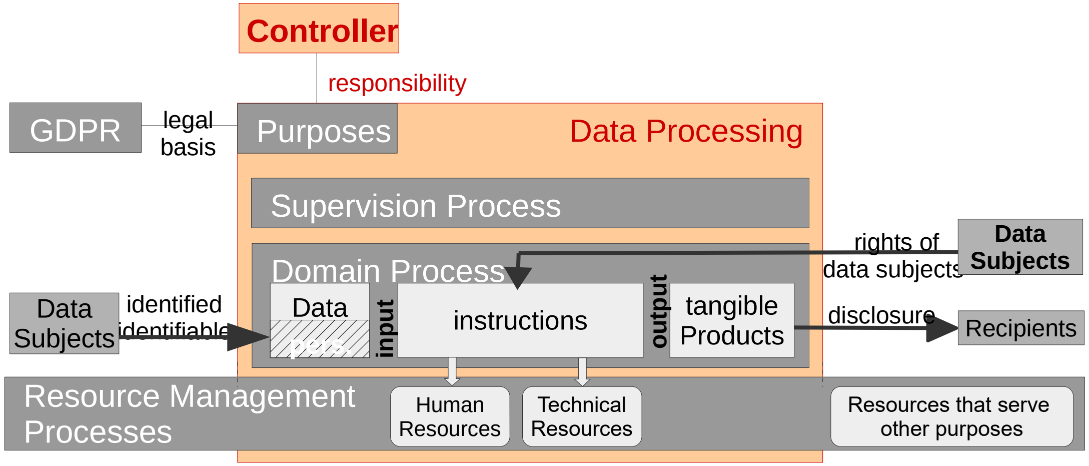
- Different types of TOMs
- Difference between IT Security and DP
- Definition of Life Cycle Phases
- Data Protection by Design: what to do in a given phase?
- How to structure documentation
- Structure the Catalog of Measures (Maßnahmenkatalog)
- …
- Wizard for DPIA

The GDPR's Model of Data Processing
(simple version)



Resources can be provided by the Controller and/or Processors

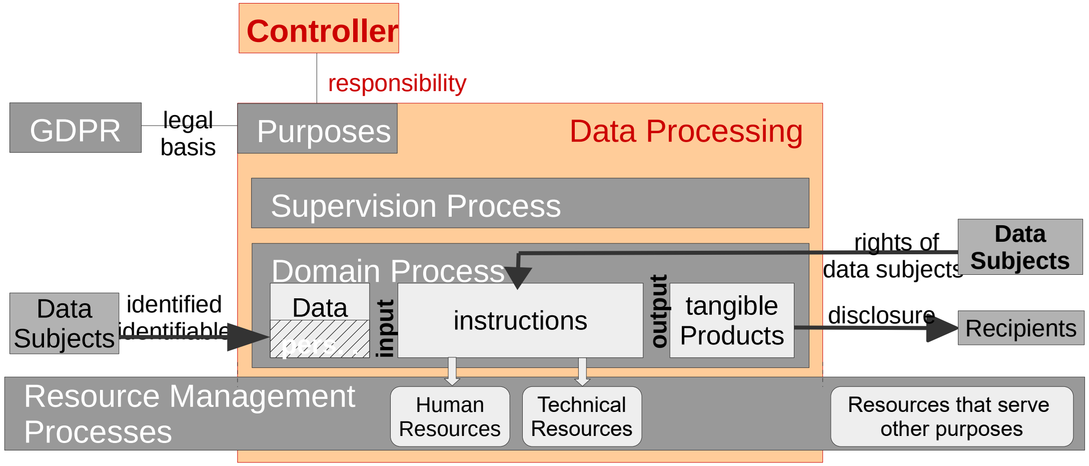
Responsibility of the Controller



Resources can be provided by the **Controller** and/or **Processors**

- Data Processing happens under the responsibility of the Controller
  - Art. 4 (7) ‘**controller**’ means the **natural or legal person** .. which .. **determines the purposes and means of the processing** of personal data;

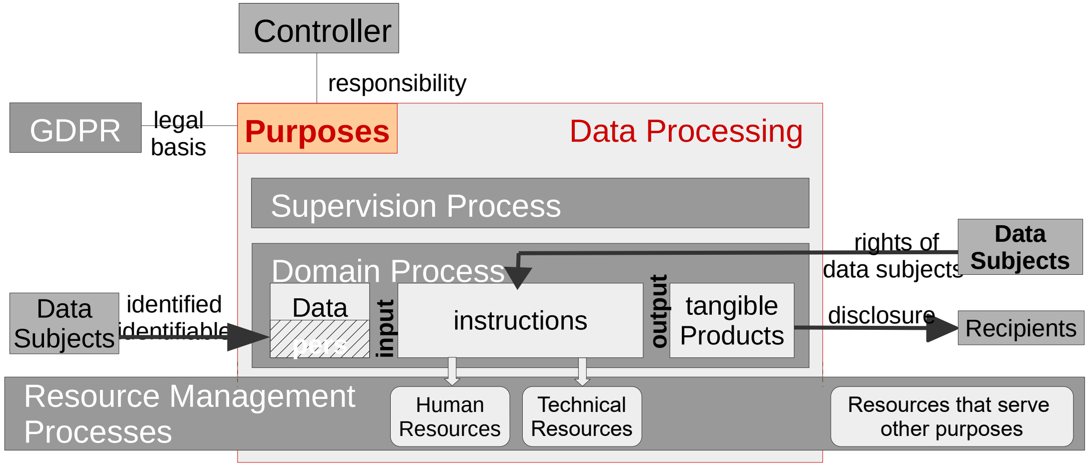
Controller is accountable for Data Protection



Resources can be provided by the
Controller and/or **Processors**

- Article 5: „*Principles relating to processing of personal data*"
  - (2) The controller shall be **responsible for**, and be **able to demonstrate compliance** with, paragraph 1 (‘accountability’).

Purposes define Processing



Controller

responsibility

GDPR

legal basis

Purposes

Data Processing

Supervision Process

Domain Process

rights of data subjects

Data Subjects

Data Subjects

identified identifiable

Data

pers

input

instructions

output

tangible Products

disclosure

Recipients

Resource Management Processes

Human Resources

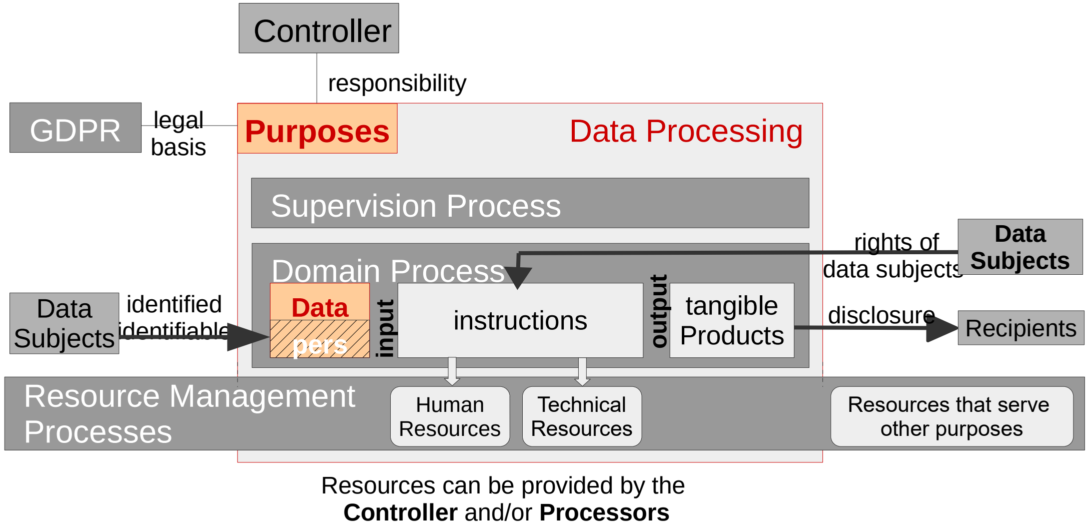
Technical Resources

Resources that serve other purposes

Resources can be provided by the **Controller** and/or **Processors**

- Purposes are the defining property of data processing
  - everything inside the Data Processing box is necessary to fulfill the purposes

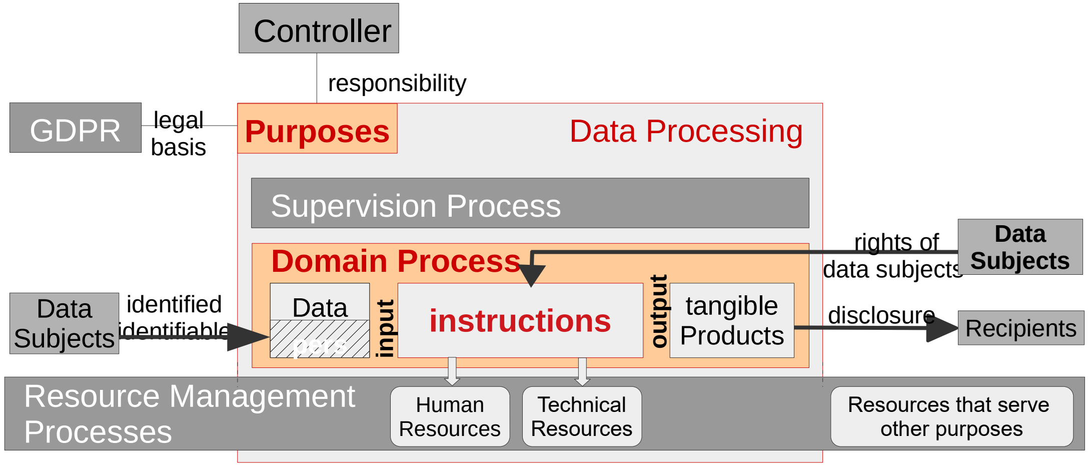
Purposes define Data Processing (1)



Resources can be provided by the **Controller** and/or **Processors**

- Art 5 Personal **data** shall be:
  - (1)(b) **collected for specified, explicit and legitimate purposes**.. ('purpose limitation')
  - (1)(c) **adequate, relevant** and **limited** to what is **necessary** in relation to the **purposes** ('data minimisation')

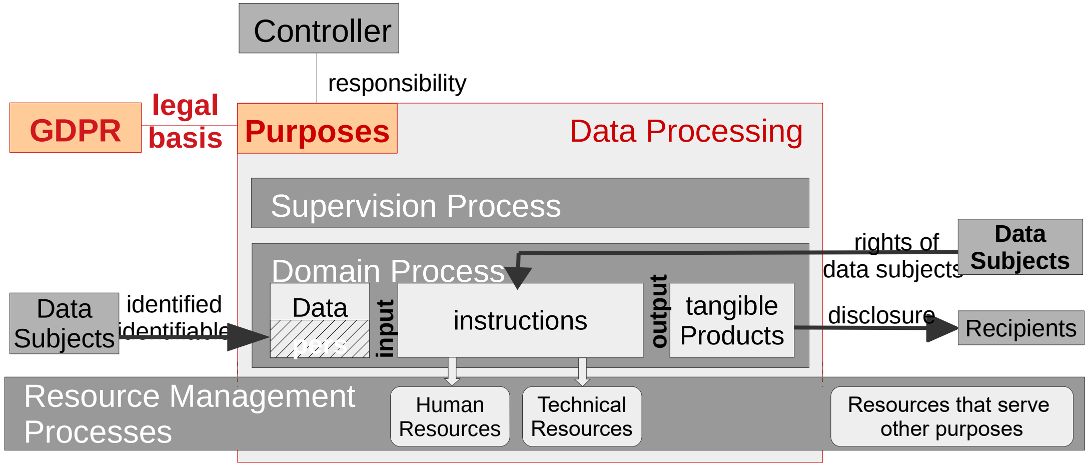
Purposes define Data Processing (2)



Resources can be provided by the **Controller** and/or **Processors**

- Art 5 Personal **data** shall be:
  - (1)(b) ..and **not** further **processed** in a manner that is **incompatible with those purposes**

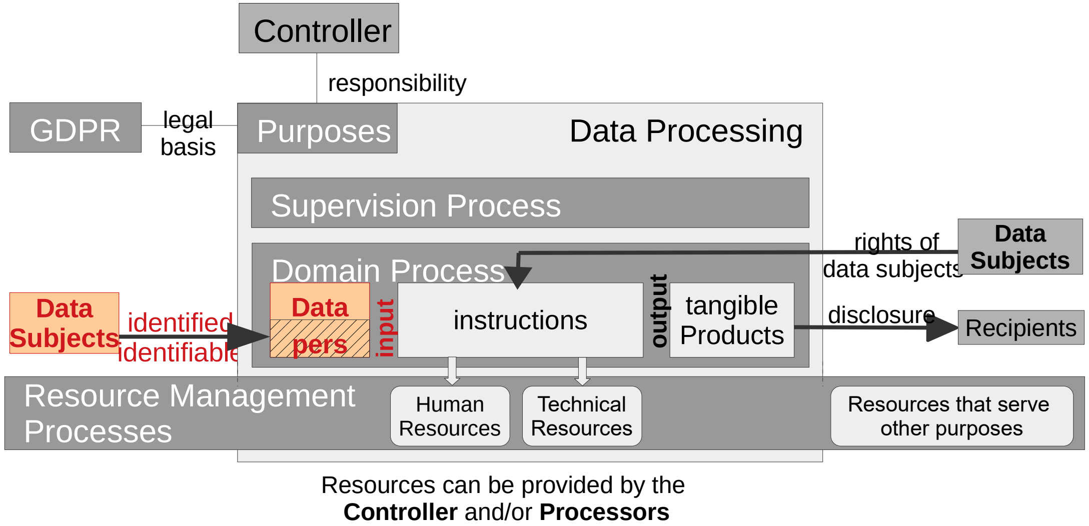
Processing shall be legitimate



Resources can be provided by the
Controller and/or **Processors**

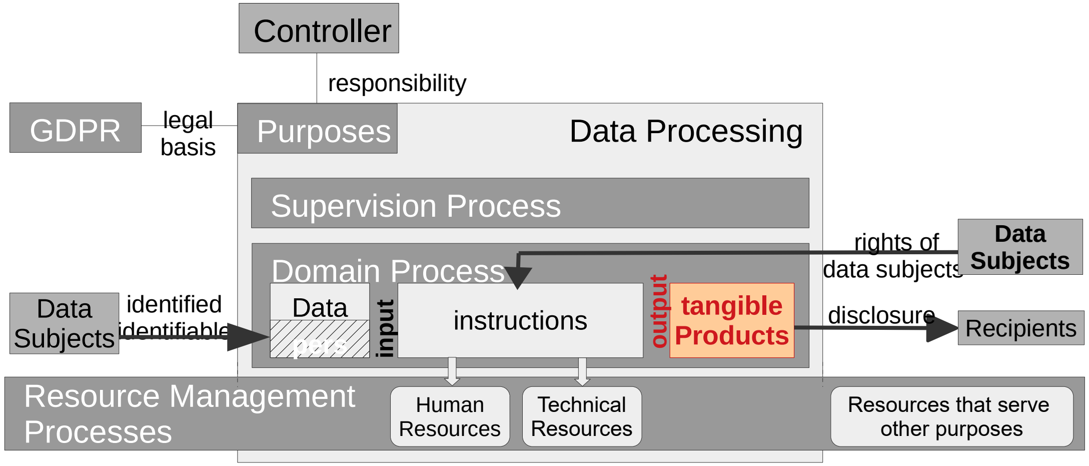
- Art 5 Personal **data** shall be:
  - (1)(a) processed **lawfully**, fairly and in a transparent manner in relation to the data subject (‘**lawfulness**, fairness and transparency’);

Personal Data



- Article 4 ‘**personal data**’ means any information relating to an **identified or identifiable** natural person (‘**data subject**’)

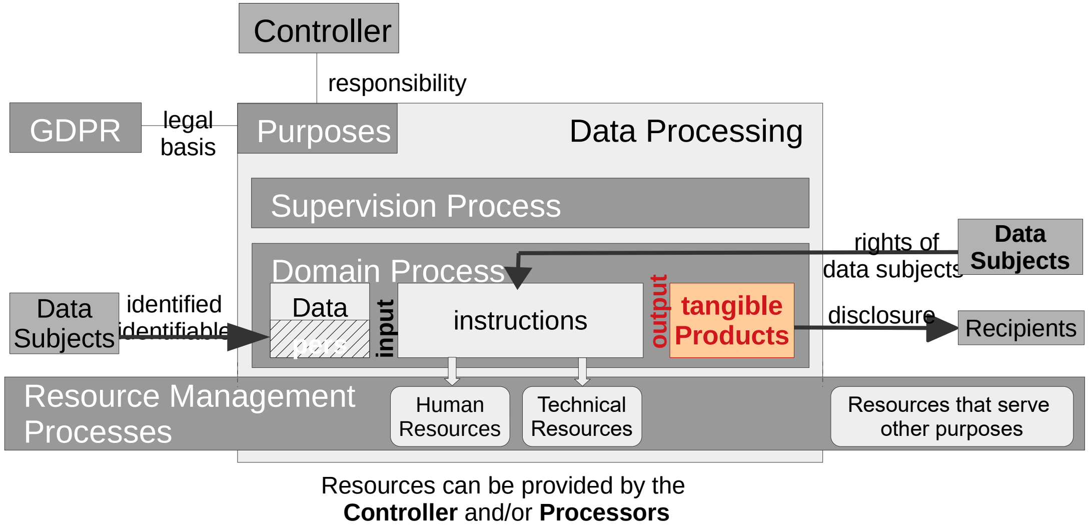
Tangible Products *(output)*



Resources can be provided by the **Controller** and/or **Processors**

- How is the Data Processing intended to affect the World?
  - **Concrete implementation of Purposes**
- Lacks Basis in GDPR
  - closest: „the **nature** of processing“ (e.g., Art 24)
- Difficult for Lawyers?

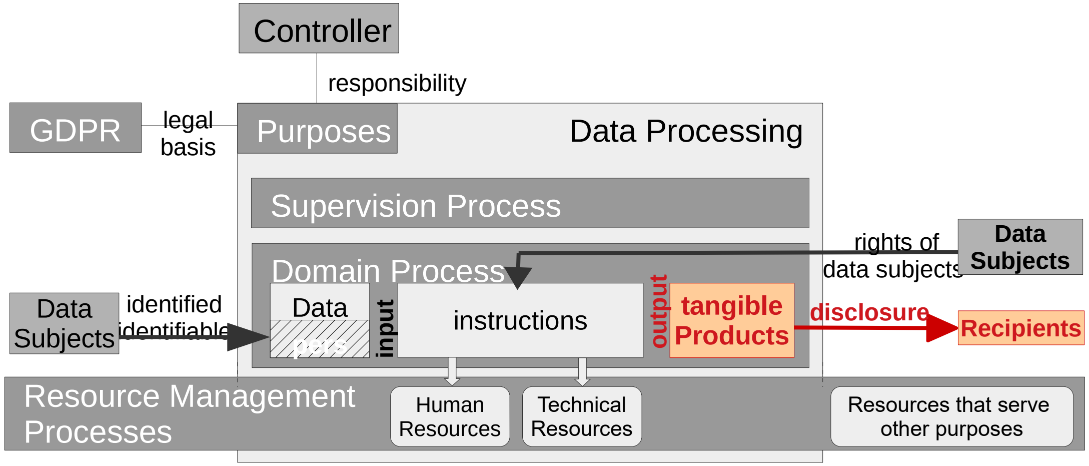
Types of Products (the Nature of processing)



- Provide **Information**
- **Evaluation** of persons (Scoring, Profiling, provide Status or Entitlement)
- **Attestation** of Information (assertions, certificates)
- Provide an **Address** to a person
- **Manage virtual resources** (bank account, property register)
- **Control of physical artefacts** (cyberphysical systems)

Gaps?
Sources?
Suggestions?

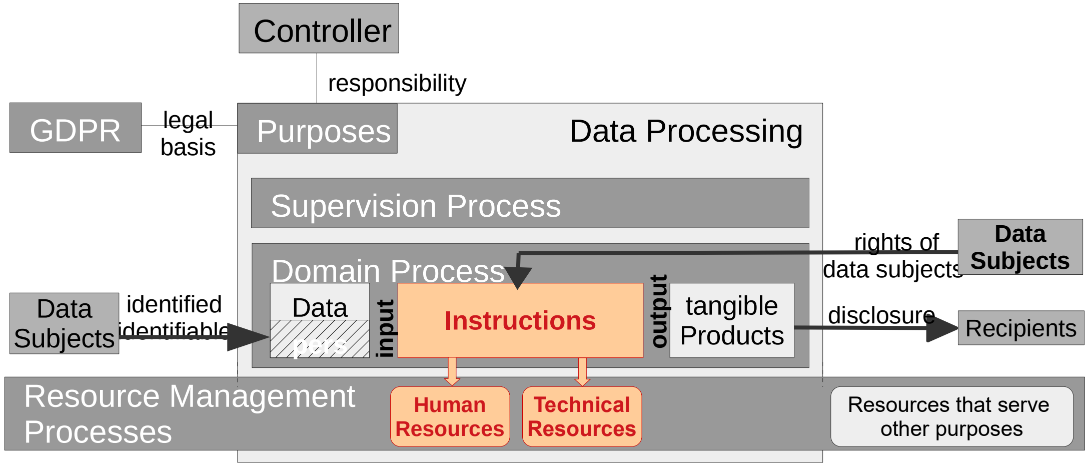
Disclosure of Data to external Recipients



Resources can be provided by the **Controller** and/or **Processors**

- The GDPR is concerned with the disclosure of data to third party recipients.

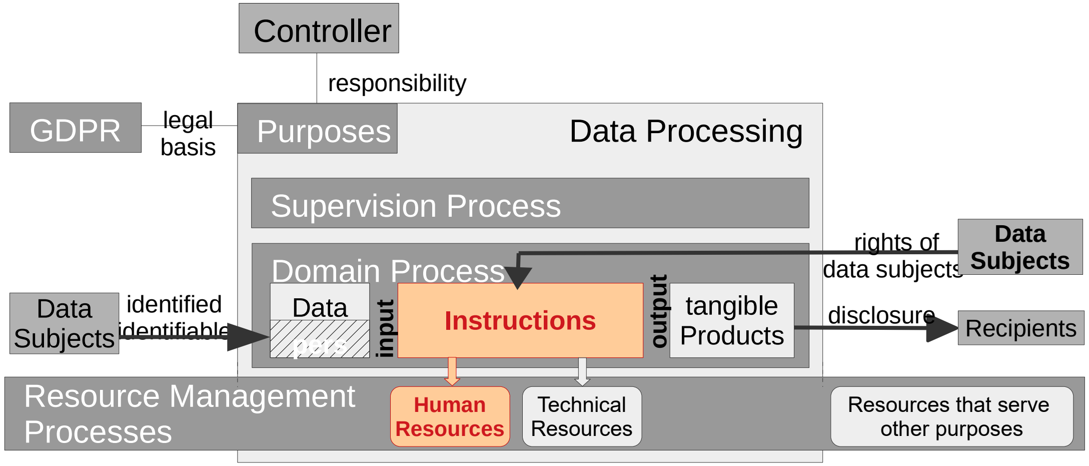
Instructions



Resources can be provided by the
Controller and/or **Processors**

- Data Processing is executed by **resources** on **instructions** from the controller
- Data Longman Dictionary: https://www.ldoceonline.com/dictionary/instruction
  - **instruction**:
    - a statement telling someone what they must do
  - **on somebody’s instructions**:
    - having been told by someone to do something

Instructions (in GDPR)

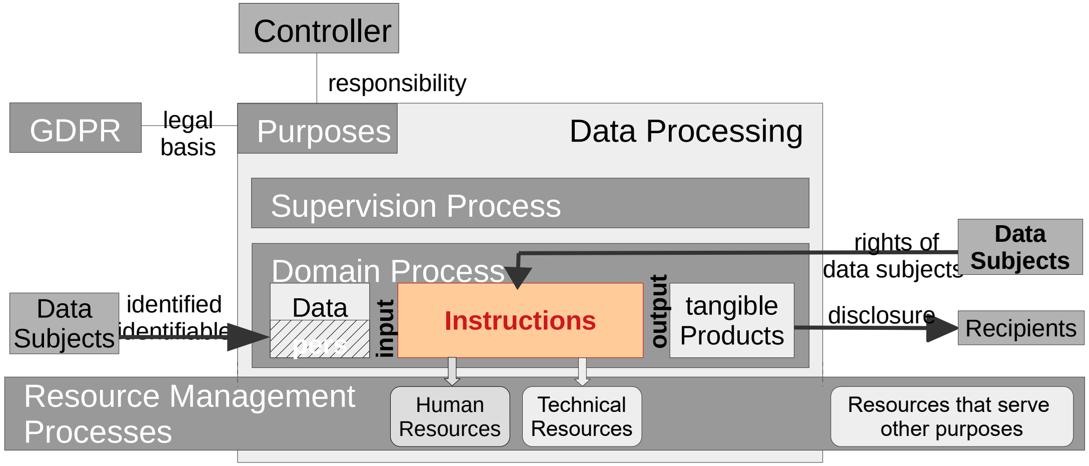


Resources can be provided by the **Controller** and/or **Processors**

- Art. 32(4) **The controller and processor** shall take steps to **ensure** that **any natural person** [Human Resource] **acting** under the authority of the controller or the processor who has access to personal data does not process them except **on instructions from the controller**..

- Art. 28(3)(a) **The Processor processes** the personal data only **on *documented* instructions from the controller..**

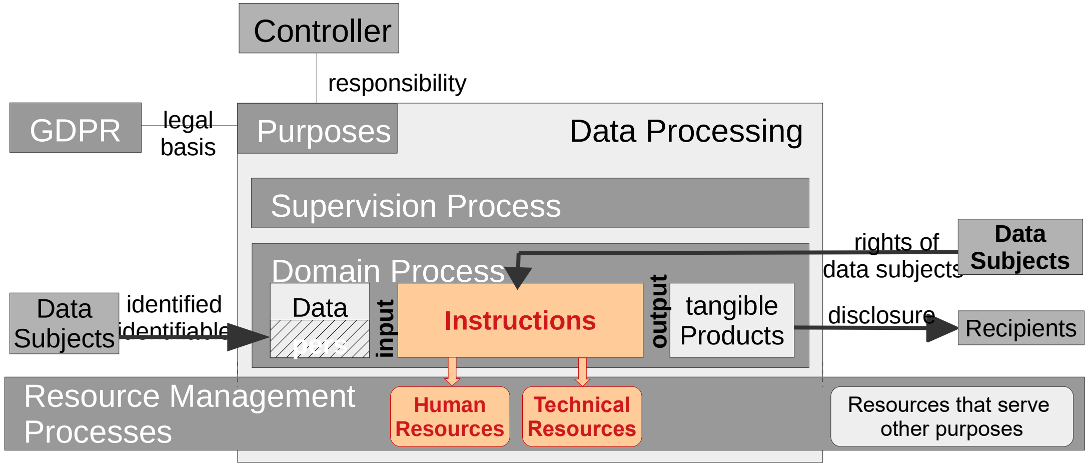
Instructions (technical interpretation)



Resources can be provided by the **Controller** and/or **Processors**

- Instruction cover the **domain** (business) **logic** of the data processing
  - They implement the purposes
  - They access data
  - They produce tangible Products
  - They instruct resources

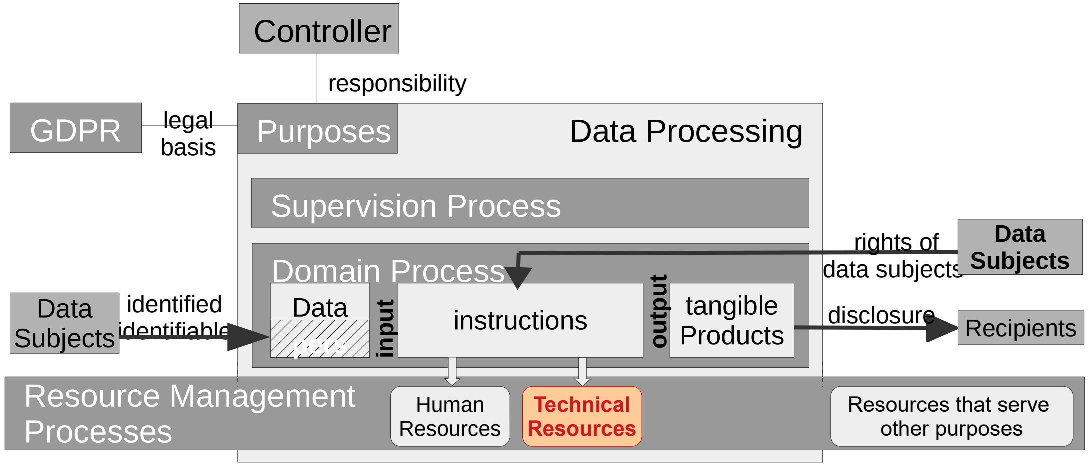
Instructions for Resources



Resources can be provided by the **Controller** and/or **Processors**

- Instructions for **Human Resources**:
  - Task description, work flow, formal business process description
    - matches the **role** of the human resource
- Instructions for **Technical Resources**:
  - Software (machine instructions)
    - matches the **instruction set** of the technical resource

Examples of Technical Resources



Resources can be provided by the **Controller** and/or **Processors**

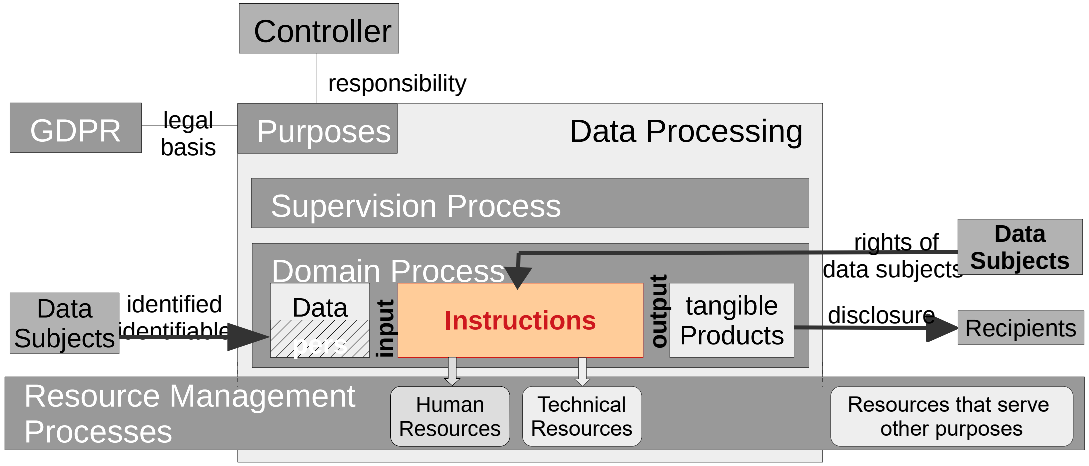
General Purpose Resources

- Windows Server
- Linux Server
- Android Device
- Google AppEngine

More Specialized Resources:

- RDBMS Server
- J2EE Servlet or Enterprise Bean Container
- J2EE Enterprise Bean Container
- Message Queue Server
- LAMP Server (Linux, Apache, MySQL, PhP)

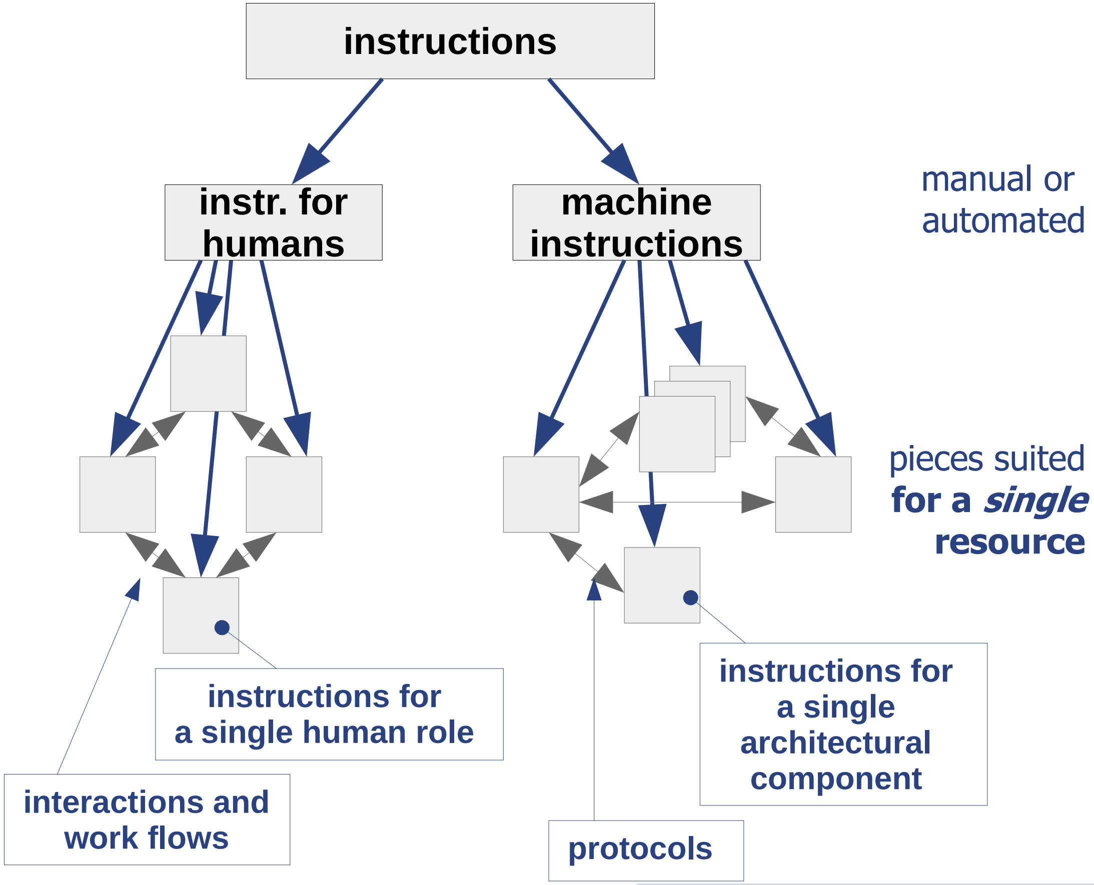
Recursive Breakdown of Instructions



Resources can be provided by the **Controller** and/or **Processors**

- **recursive breakdown**
  - as common in Organization and Informatics
  - sequential and/or parallel
  - separate instructions for humans and for machines
  - architecture as breakdown: units of instructions suitable for a single resource

Recursive Breakdown of Instructions



instructions

instr. for humans

machine instructions

manual or automated

pieces suited **for a *single* resource**

instructions for a single human role

interactions and work flows

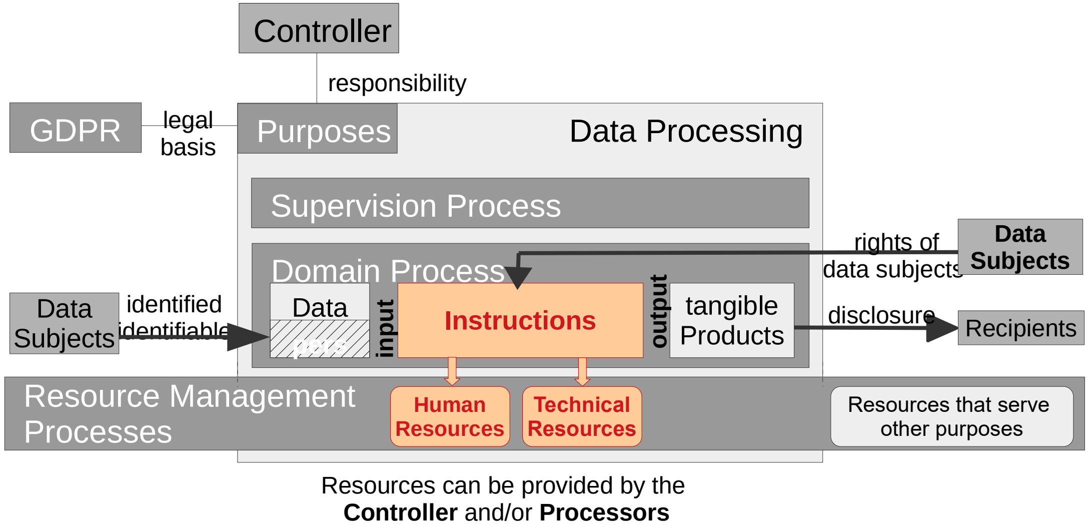
instructions for a single architectural component

protocols

Responsibility and line of command

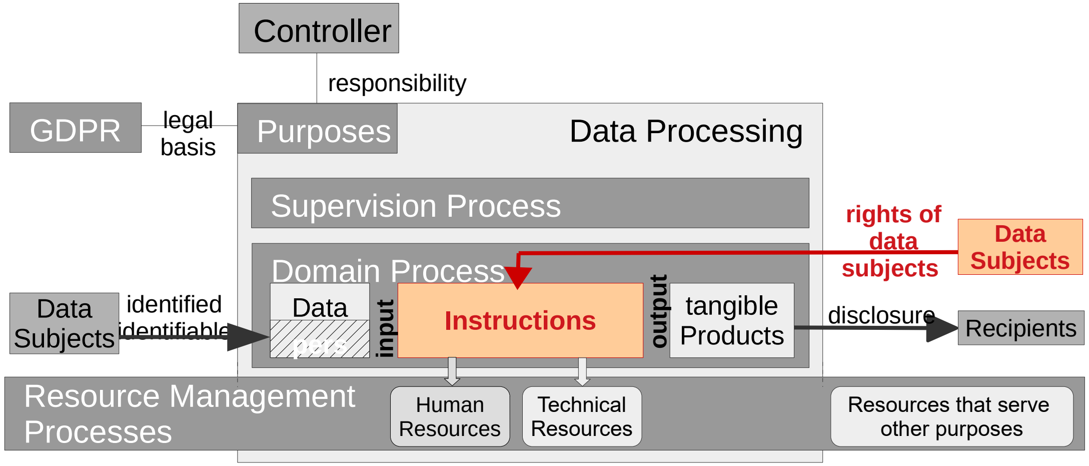
- **The Controller is responsible for every aspect of data processing**
  - processors act only on (written) instruction of the controller
  - Human Resources only act on instruction of the controller
  - Technical Resources are always controlled by Humans:
    - approve (by controller)
    - install
    - configure
    - run
- There is an **uninterrupted line of command** from the controller to any action by any resource

Terminology: Processing Operations



- Operation = Execution of Instruction by a Resource
  - acting on concrete data
  - procuding concrete products

Rights of Data Subjects



Controller

responsibility

GDPR

legal basis

Purposes

Data Processing

Supervision Process

rights of data subjects

Data Subjects

Domain Process

Data Subjects

identified identifiable

Data

pers

input

Instructions

output

tangible Products

disclosure

Recipients

Resource Management Processes

Human Resources

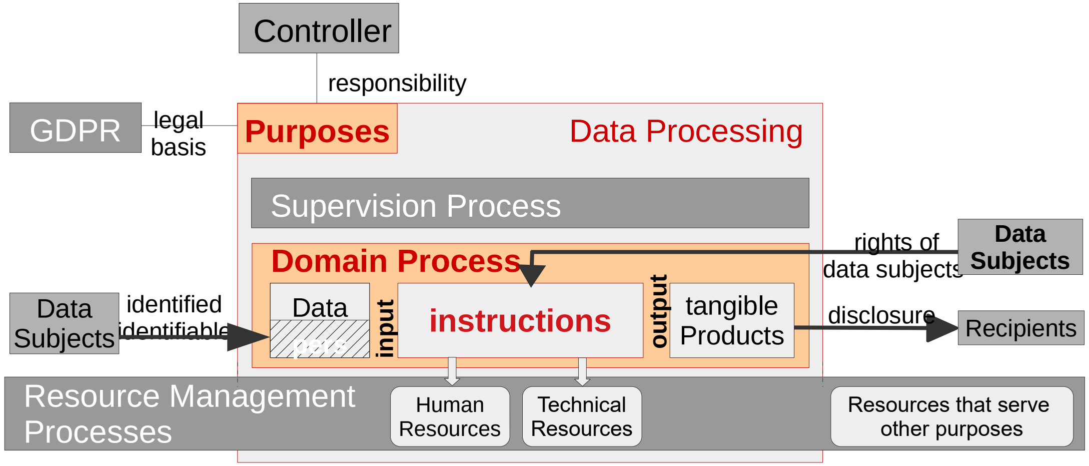
Technical Resources

Resources that serve other purposes

Resources can be provided by the **Controller** and/or **Processors**

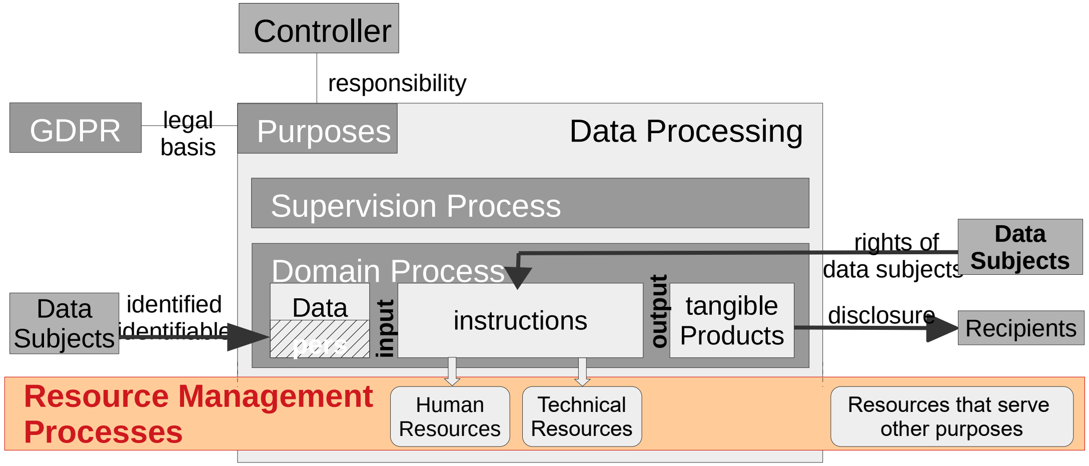
- Data Subjects have the Right to give instructions that are executed by Resources:
  - access to and download of (data portability) own data
  - rectification, erasure, restriction, objection, withdrawal of consent
- This requires **Access Control**

The Domain Process is specific to the Purposes



Resources can be provided by the **Controller** and/or **Processors**

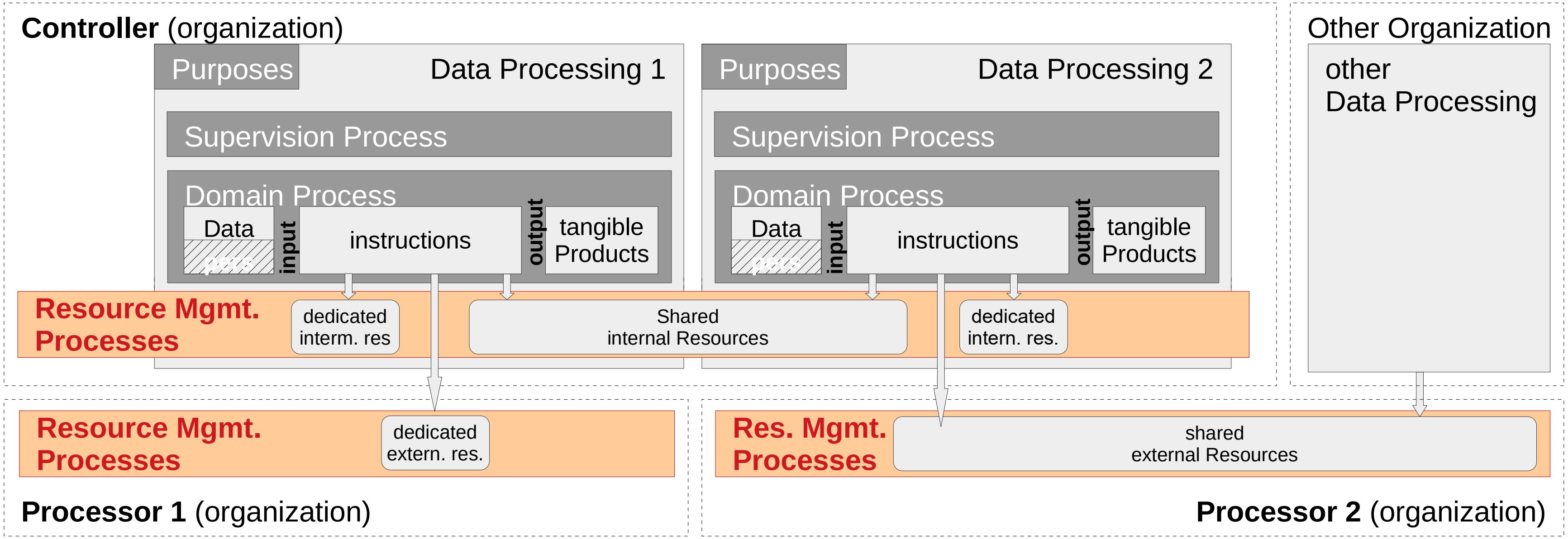
Resource Management Processes *are not specific to the purposes*



Resources can be provided by the **Controller** and/or **Processors**

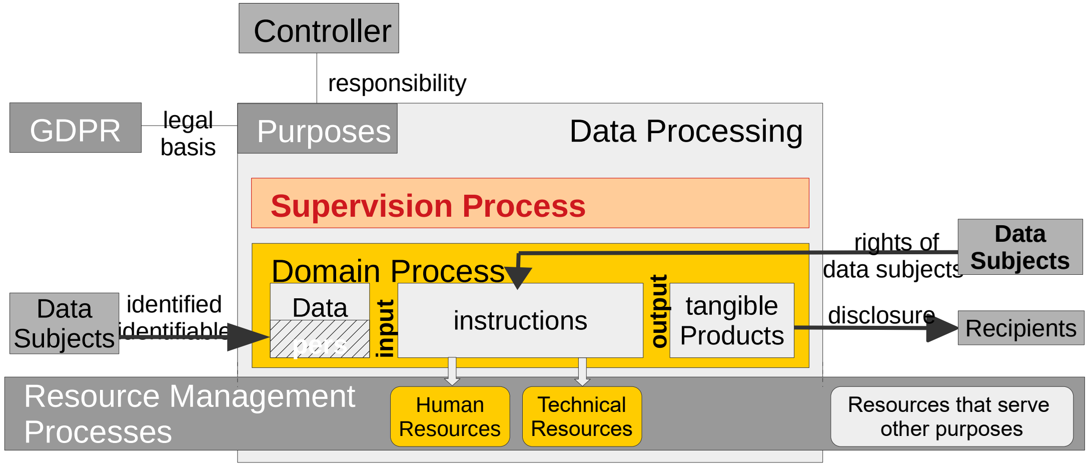
- Human Resource Department
- IT Department
  - both are **not specific to the purposes** of processing
  - therefore reaches outside of the „Data Processing" box

Resource Management Processes in Detail



- Resources can be provided
  - by the **controller** (**internal** resource)
  - by one or several **processors** (**external** resource)
    - Processors can further subcontract other processors to provide resources
- Resources can be **dedicated** to a specific data processing/purpose or **shared**

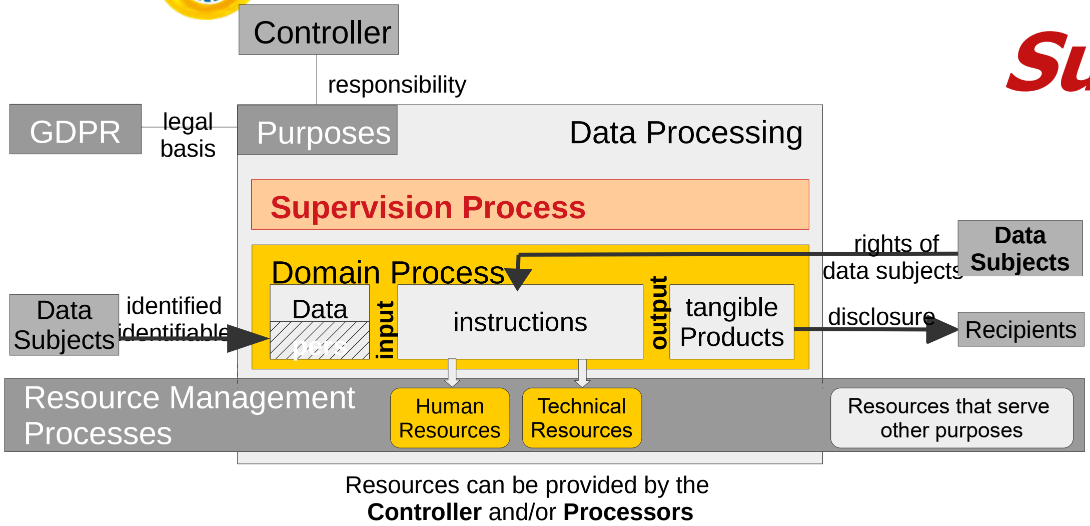
Supervision Process



Resources can be provided by the **Controller** and/or **Processors**

- Process to supervise processing operations
  - execution of instructions by resources
  - Detect exceptional conditions
  - Intervene to return to normal conditions

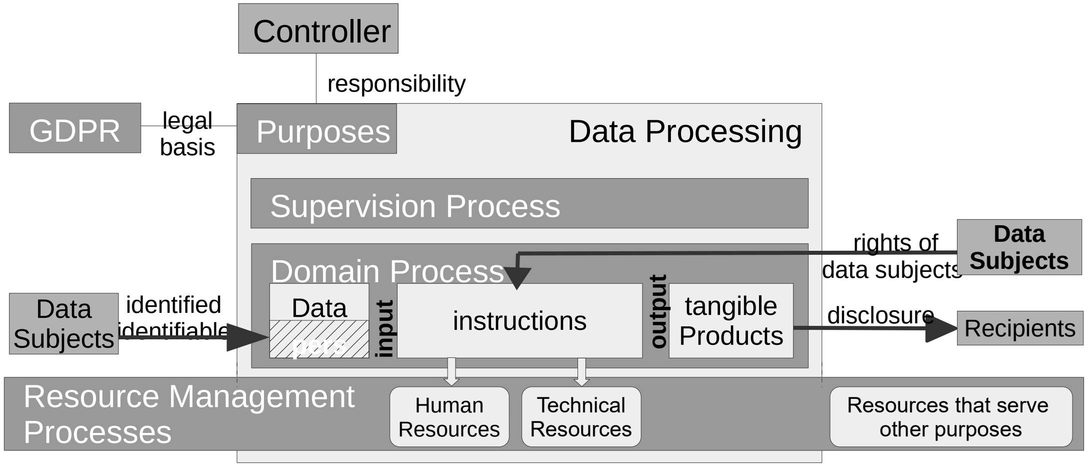
Supervision Process
Basis in GDPR



Resources can be provided by the **Controller** and/or **Processors**

- Art 32(1)(d) [the controller and the processor shall implement appropriate technical and organisational measures, including] a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- Art 33 and 34: Detect breaches and notify/communicate to supervisory authority/data subject
- Art 28(3)(h) inspections of processor conducted by the controller
- Art 32(1)(b) "resilience": "gracefully manage the unforeseen"
- Art 25(1): Data Protection by Design: „at the time of the processing itself“

A Model of Data Processing for the GDPR



Resources can be provided by the **Controller** and/or **Processors**

- **Data Processing** is represented by a box.
- The content of this box is guided by the **purposes**.
- A **controller** is responsible for the data processing.
- The data processing has a **legal basis.**
- The **domain process** implements the purposes. (Domain Logic, business logic)
- It accesses **data**, part of which are personal and thus relate to **data subjects**.
- The **outputs** and tangible effects on the world of the processing is expressed by **products**.
- The processing is executed by **human** and **technical resources** following **instructions** from the controller.
- **Data subjects** have the **right** to influence the processing and trigger operations such as deletion.
- One or several **resource management processes** (e.g. an IT department) provide the necessary resources.
- A **supervision process** monitors operations and intervenes when necessary. (E.g. the notification of breaches)

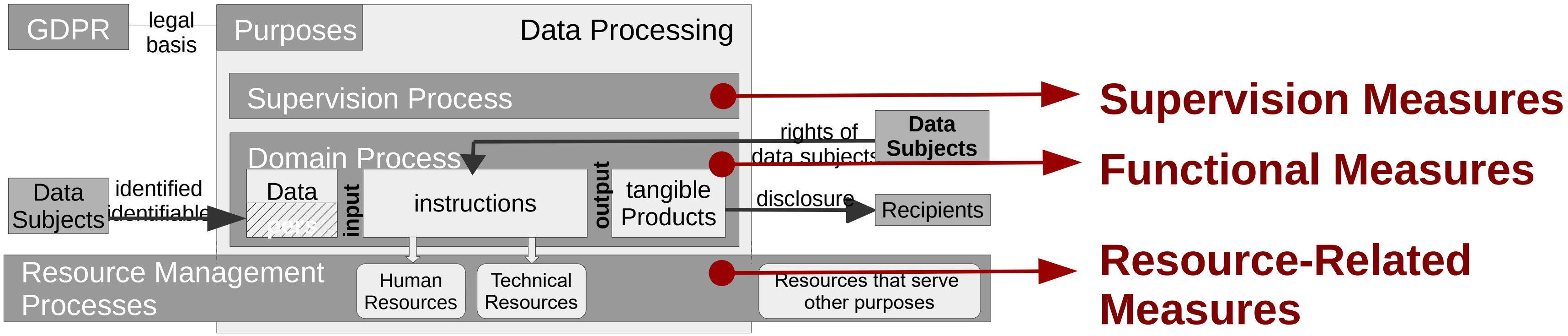
Discussion

Application Example

- optional

(TOMs) Technical and Organisational Measures

THE way to comply with data protection



Resources can be provided by the **Controller** and/or **Processors**

- Art 24(1) ..the **controller shall implement appropriate technical and organisational measures** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation..

- Art 28(1) ..the controller shall use only **processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation

Deployment-time TOMs

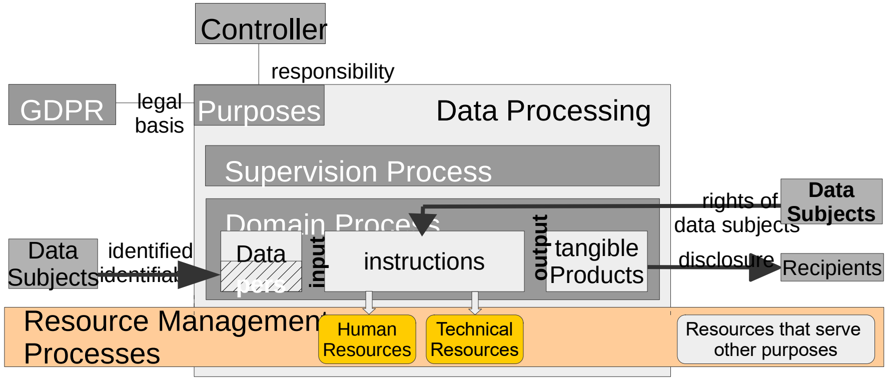
Risk Thinking

Assumptions about Resources:

- behave only as instructed
- unaffected by instructions of other purposes (isolation)

Undesireble Events affect Resources

- **likelihood** << 100%
- **caused by**
  - **Actors** (persons, organisations): Attacks
  - **Technology**: Failures
  - **Nature**: Disasters
- **breaks assumptions about Resources**
  - Behavior deviates from instruction
    - including failure
  - Influenced by instructions for other purposes
- **causes Damage**



Resource-Related Measures:

- reduce likelyhood of occurance
- limit possible damage (Supervision)
  - detect occurance
  - intervene

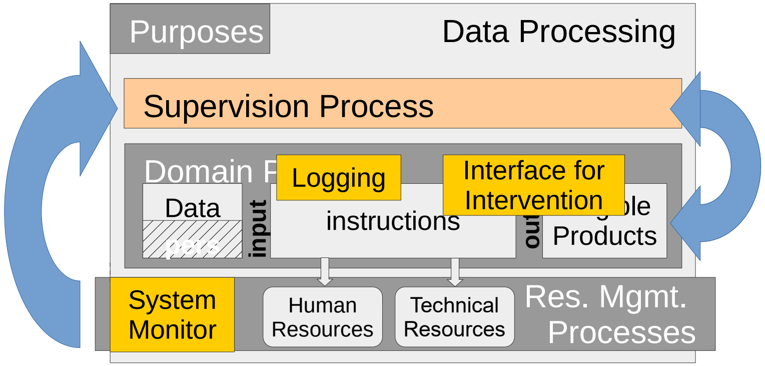
Supervision Measures

Monitoring
- audit of logs (autom./manual)
- inprections (of processor)

Intervention
- manual work around of unforseen use case
  - uses low-level DBMS interface
- install non-routine new version of SW
- fail-over to disaster recovery site
- change processor
- discipline/fire HR
- extraordinary awareness/training session

Supervision Measures:
- Monitor Processing
- Intervene when necessary

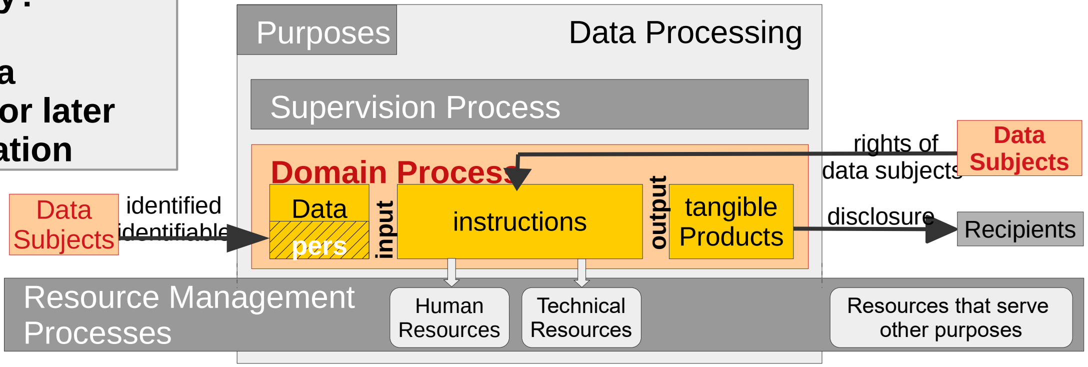
report
unmanaged
problems



- monitorable trough logging
- interfaces enables intervention

Functional Measures
TOMs in Domain Process

- Low-impact data acquisition method
- Effects of inaccuracy?
- Enroll data subjects for later authentication



- Functionality for rights of data subjects
- Authentication of data subjects

- Architecture:
  - patterns and anti-patterns
    - avoid centralized big brother components
    - privacy friendly protocols
- Implementation:
  - **Storage Management** (Deletion!!!)
  - **Access Control for Human Resources**
  - Monitorable (Logging, Monitoring Interfaces, ..)
  - Intervenable (direct DBMS interface, ..)
  - Integrity by Design (transactions)
  - Confidentiality by Design
  - Availability / Resilience by Design

unlinkability

other 5 standard protection goals

Least Understood!
Structure?
Ideas?