SWISS MEDTECH

AI LEGAL
& STRATEGY
CONSULTING AG.

Swiss data protection

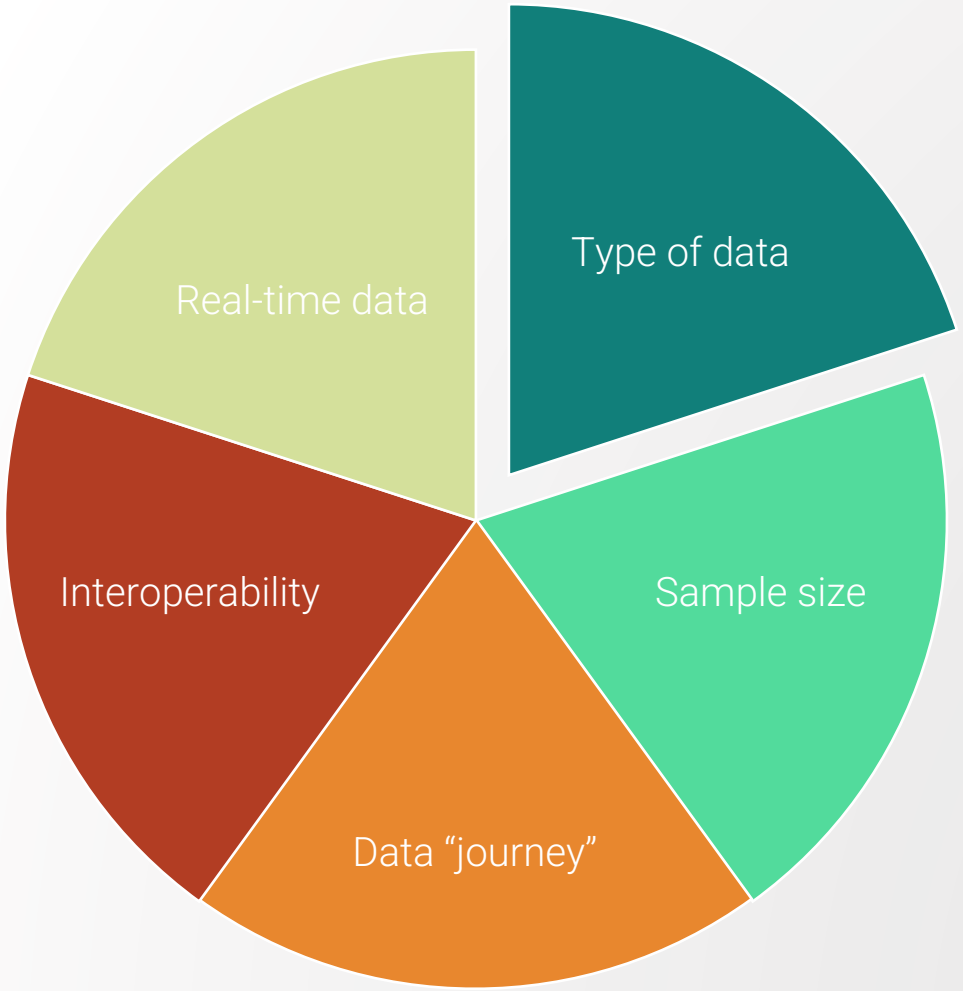
What’s in store for me, what do I have to do?

Agenda

- Dealing with data in Medtech sector
- Why a total revision of the law?
- GDPR v. new DPA
- General approach - Practical advice
- New concepts
- Actions to be taken

Dealing with data in the MedTech sector

A few particularities



Why a total revision of the law?
Equivalence

European Union (GDPR)

Preserve the compatibility of Swiss law with EU law

Grant new rights to Swiss citizens

Switzerland

DPA underwent total revision

Associated ordinances had to be amended:

- Ordinance to the Federal Act on Data Protection
- Ordinance on Data Protection Certifications

What does it mean?
developments

General improvement of transparency

Increased supervisory powers and independence of the FDPIC

Strengthening of criminal law provisions

Privacy by design and privacy by default

Obligation to carry out impact assessments on personal data

The right to data delivery and portability

Promoting data security and reporting data breaches

GDPR – new DPA
key differences

European Union

Strict protection rules

Switzerland

Introduction of instruments & obligations for controllers from the GDPR

Less stringent rules

(Consent or exercise of the rights of the concerned Persons)

Stricter requirements

(Penalties)

GDPR – new DPA
key differences

European Union

Personal data

any information relating to an identified or identifiable natural person

Special categories

Switzerland

= Personal data

Relative approach

≠ Sensitive data

Risk-based approach

Anonymisation vs Pseudonymisation

Anonymisation vs Pseudonymisation

What is the difference

Anonymous

- information which does not relate to an identified or identifiable natural person

→ data protection does not apply

Pseudonymised

- information which can be (re)attributed* to a natural person with the use of additional information

→ data protection applies

* EU GDPR – theoretical risk | CH DPA – practical (current?) risk

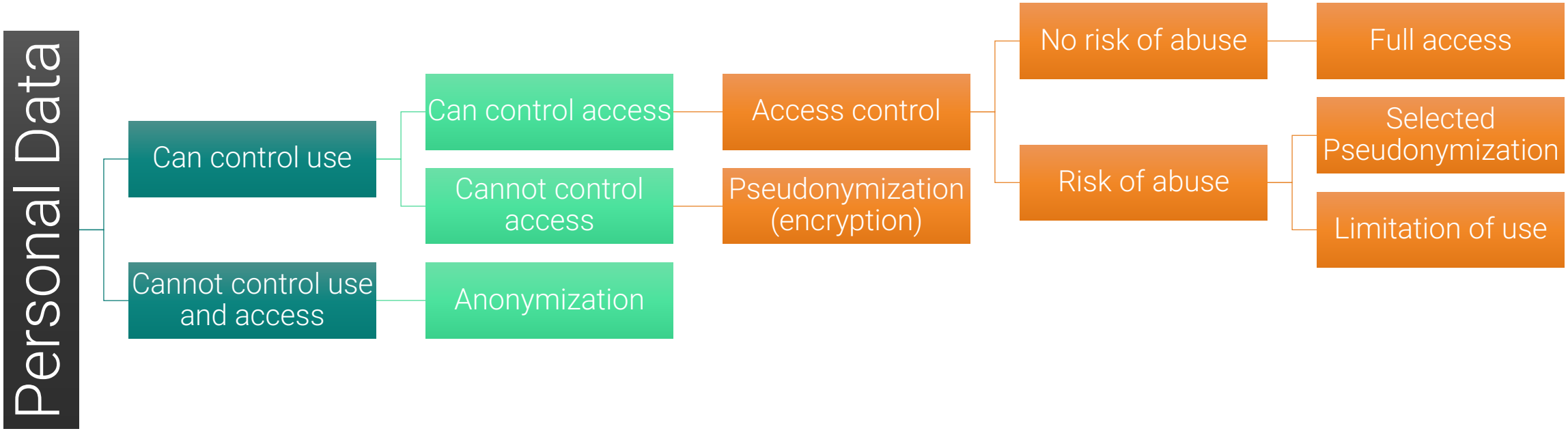
Problems

Balancing act of different requirements

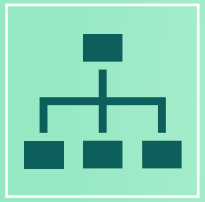
Utility vs. data protection (how much information is available and to which granularity)

Operable (calculation by computer)

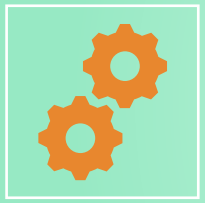
Intelligible (can be understood by user)


Personal Data
Can control use
Cannot control use and access
Can control access
Cannot control access
Anonymization
Access control
Pseudonymization (encryption)
No risk of abuse
Risk of abuse
Full access
Selected Pseudonymization
Limitation of use

2 key dimensions



Technical measures



Organizational measures

General approach
practical advice

Risk-based approach

Proportionality with respect to means

Good faith

Primarily administrative law

Understanding of purpose rather than formalism

New concepts
alignment with recognized standards

- Personal data = natural persons (Ø legal entities)
- Data controller (ex “controller of the data file”)
- Genetic and biometric data = sensitive data
- Profiling & high risk profiling
- Impact analysis
- Duty to inform extended to collection of any personal data (not only sensitive data)
- Register of processing activities
- Automated individual decision
- Rapid notification procedure in case of data security breach
- Data Protection Officer (DPO)
- Representative in case of a private data controller with headquarters or domicile abroad
- Code of conduct

Impact analysis
take stock of your activities

Description of the intended processing operation

Assessment of the risks to the data subject's personality or fundamental rights

Planned measures to protect the data subject's personality and fundamental rights

Register of processing activities
content requirements

Contains at least

- the identity of the controller
- the purpose of the processing
- a description of the categories of data subjects and of the categories of personal data processed
- the categories of data recipients

To the extent possible

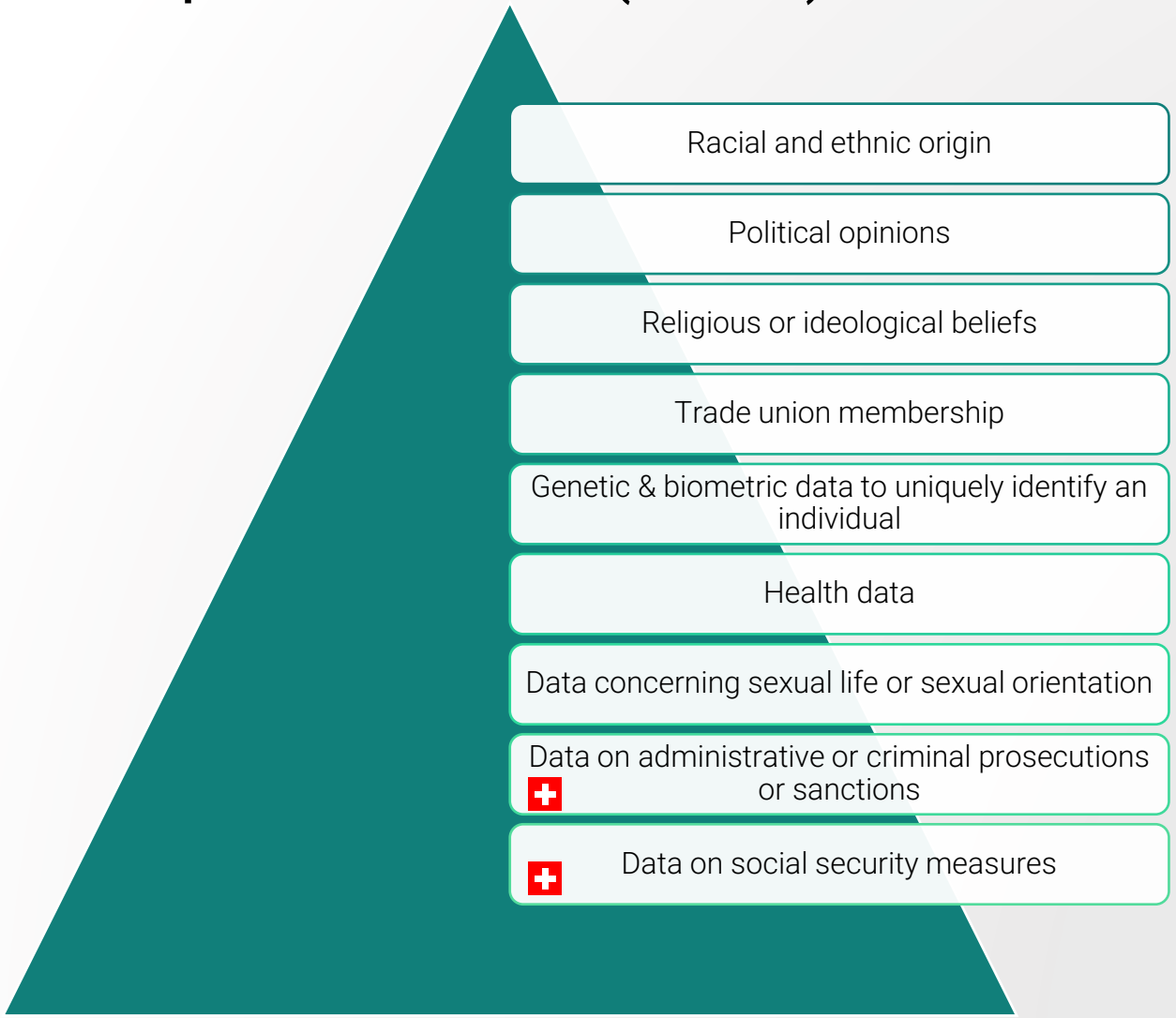
- the retention period for personal data or the criteria for deciding the retention period
- a general description of the measures to ensure data security

Where personal data is transmitted abroad

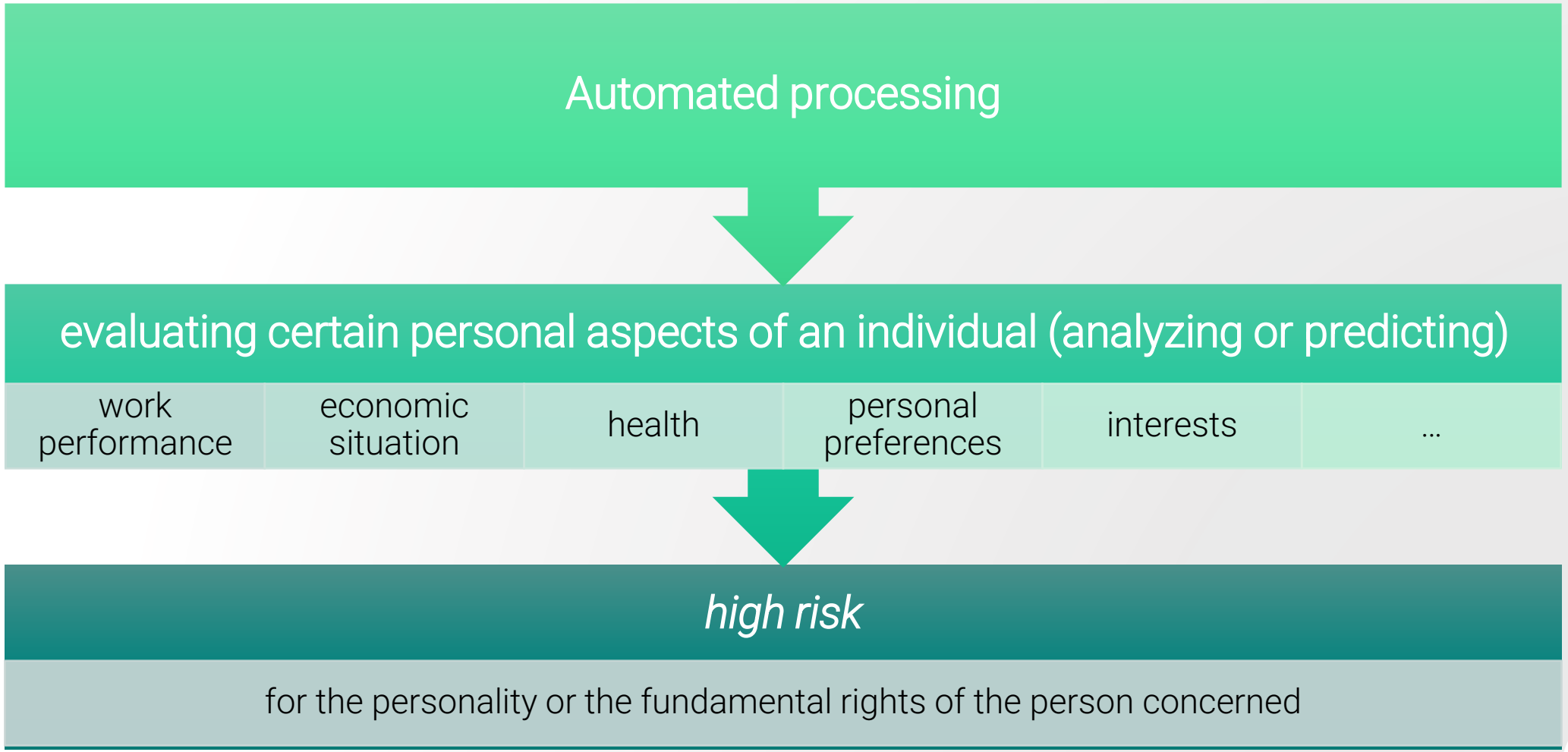
- the name of the countries concerned and the safeguards provided

Personal data requiring special protection (nDSG)

Special categories of personal data (GDPR)

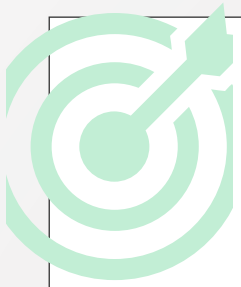


Profiling
what is it?



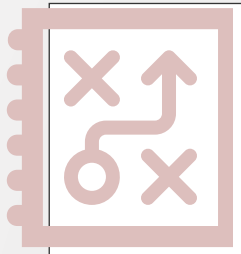
Information duties
at the time of the collection

Identity and contact details of the data controller



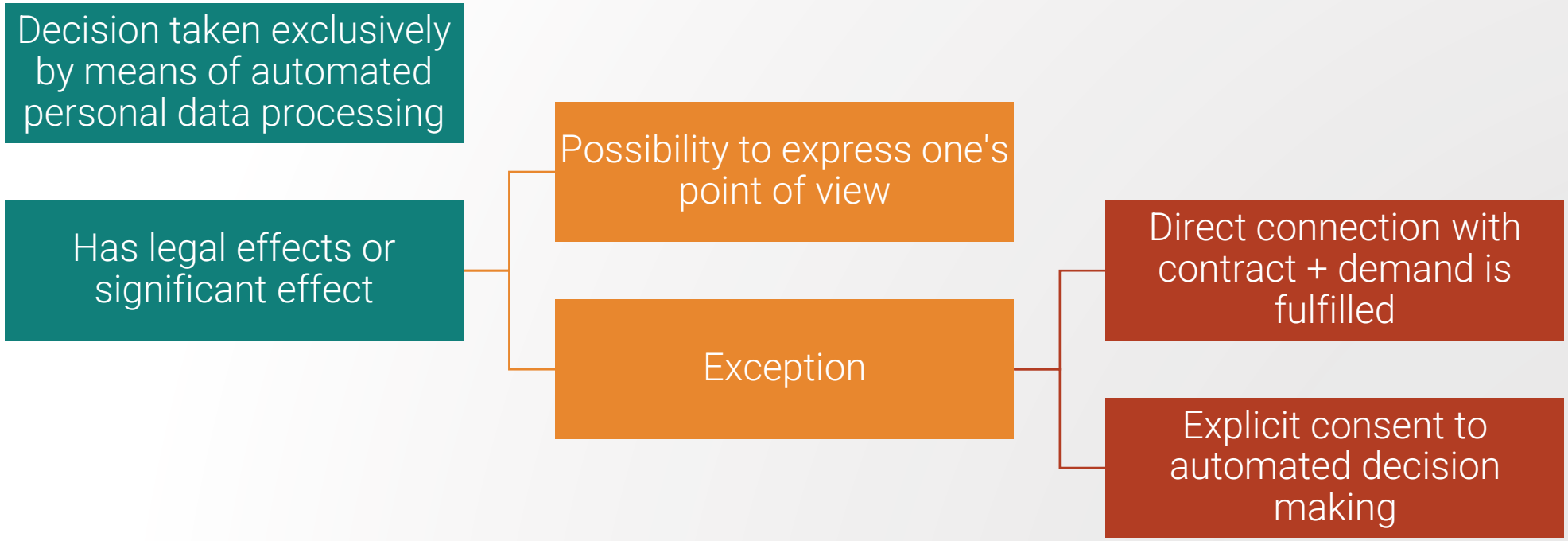
Purpose of the processing

Recipients of transferred personal data

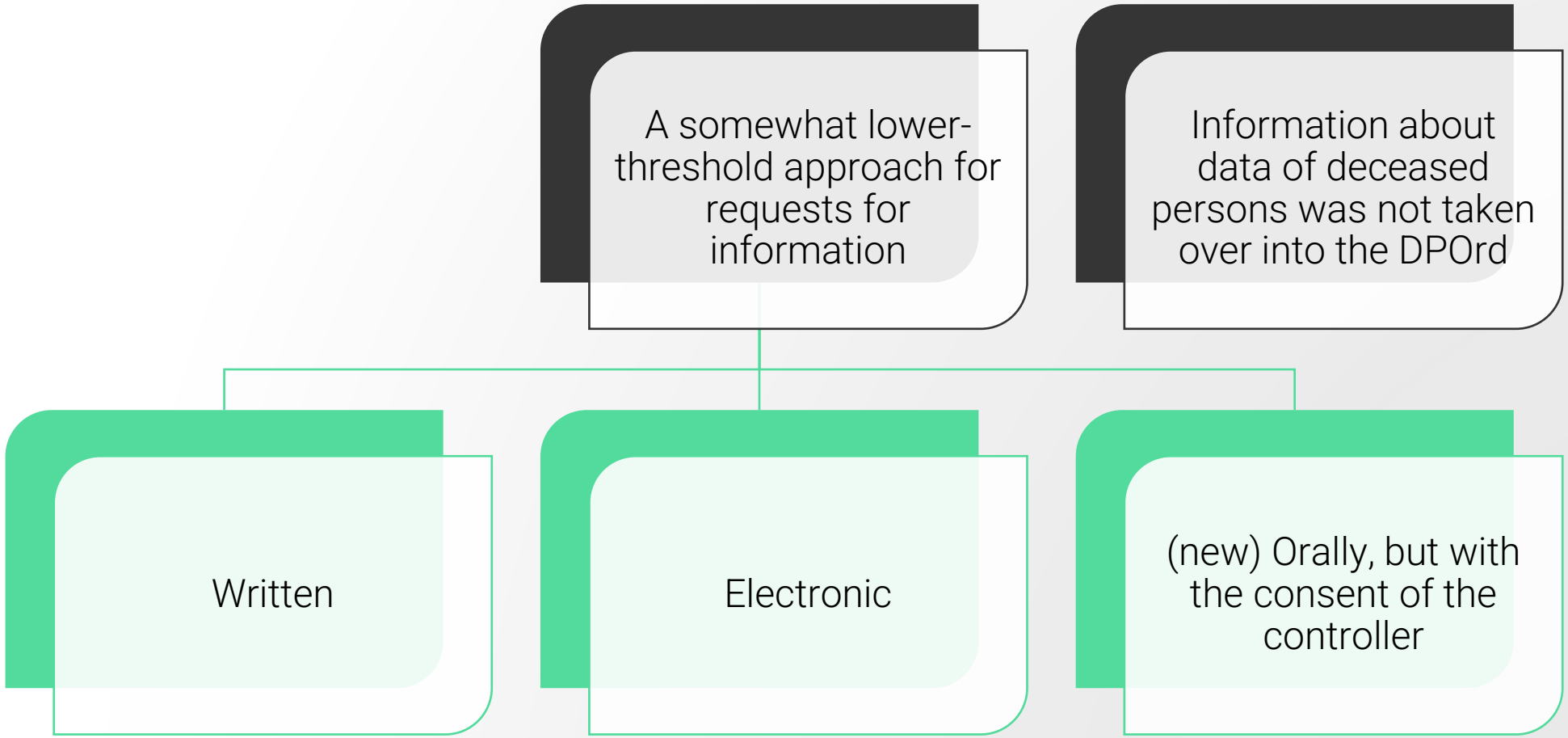


Exception?

Information duties
for automated individual decisions



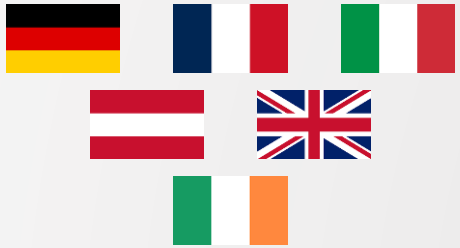
Right to information
for data subject



Transfer of personal data abroad

Adequate level of protection

List



Verify other measures

Exceptions?

& co.

Data security
principles

01

Confidentiality

is accessible only to authorized persons

02

Availability

is available when needed

03

Integrity

cannot be modified without permission or by mistake

04

Traceability

are processed in a traceable manner

Data security
logging requirement

Personal data requiring special protection is processed automatically on a large scale

or

High-risk profiling is carried out

+

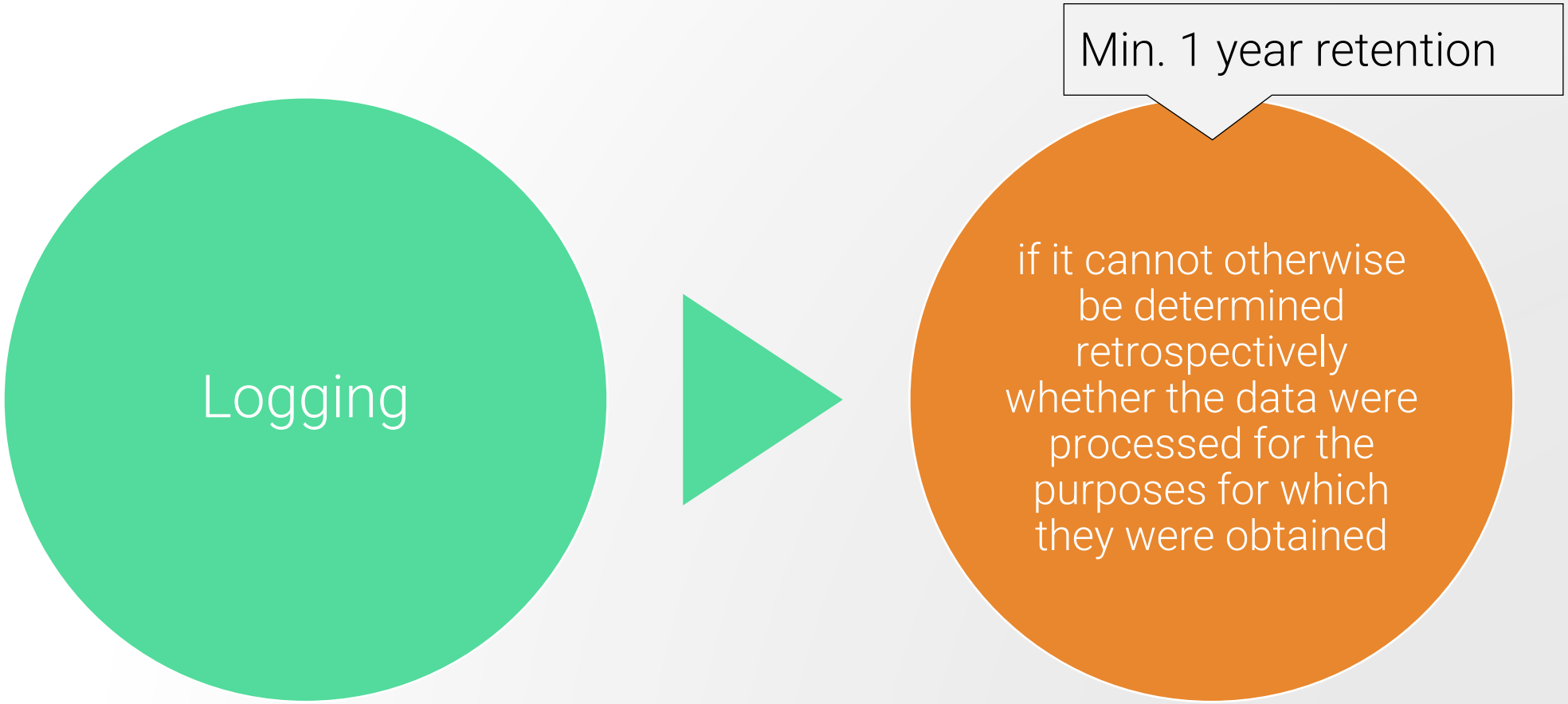
Preventive measures cannot ensure data protection

→

at least

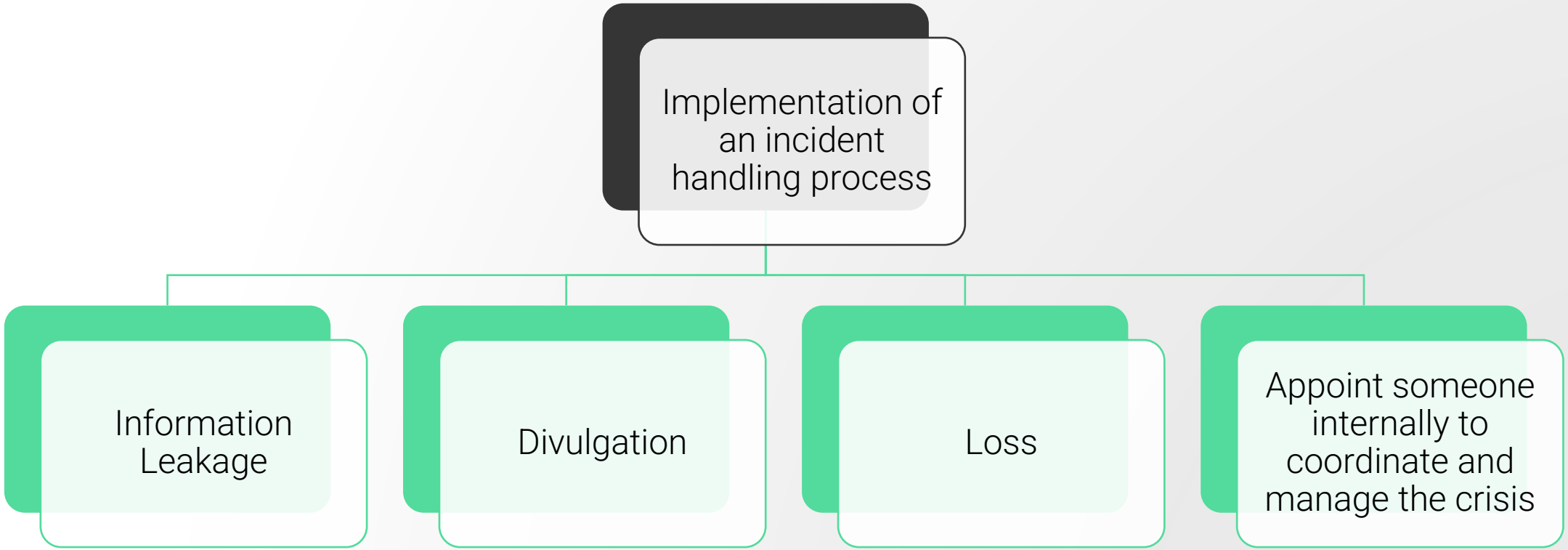
log the storage, modification, reading, communication, deletion and destruction of the data

Data security
logging purpose



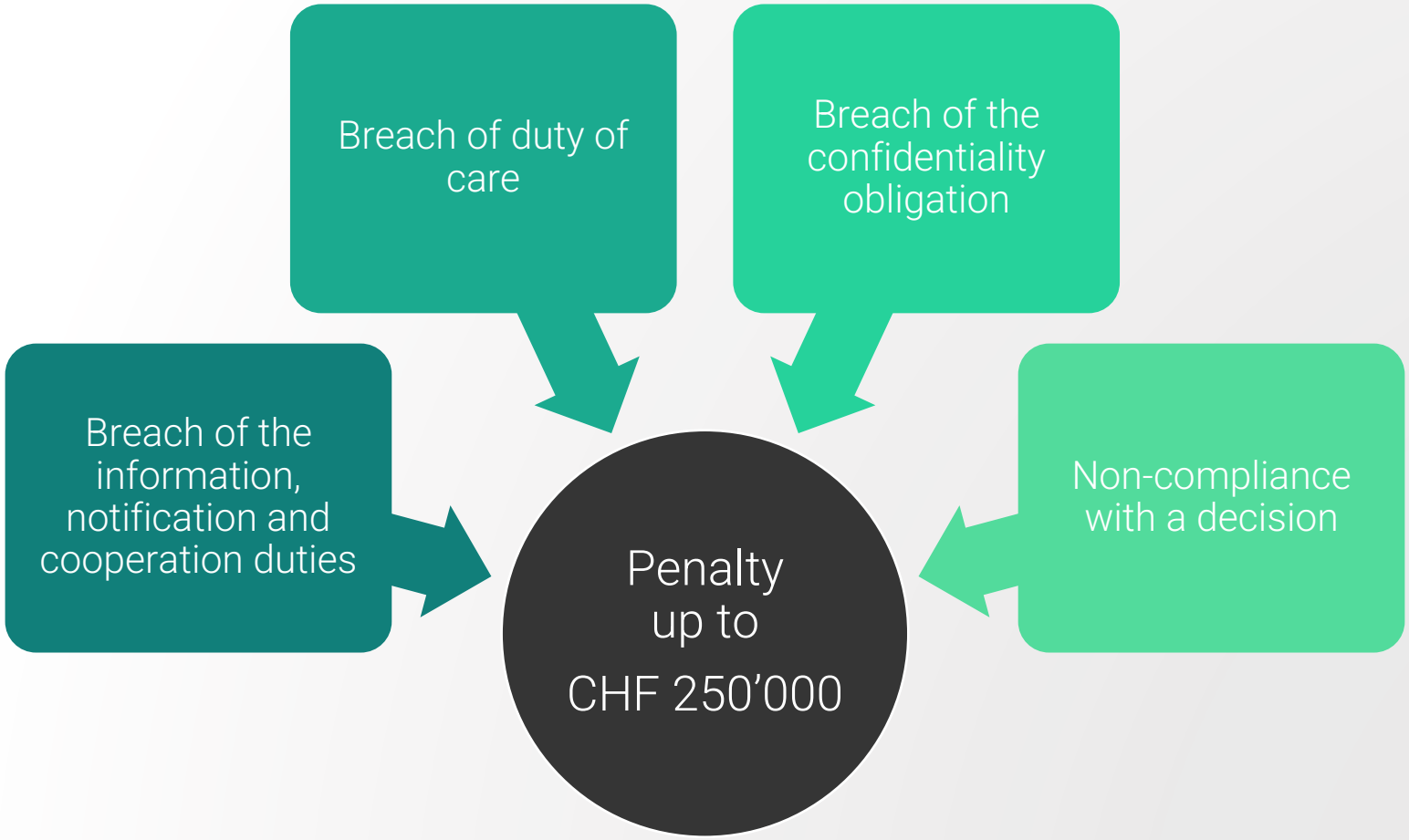
Data Processing Policy still required

Incident Handling Process
scenarios



Criminal provisions
personal impact*

* Exception possible



Actions to be taken

Internal organization - data processing

Person responsible or data protection officer

Information - contacts for nDPA requests

Disclosure of personal data to a third party or abroad

Cybersecurity, minimization and deletion of personal data

AI LEGAL
& STRATEGY
CONSULTING AG.

PRISCA QUADRONI
Lic. Iur., LL.M., Lawyer
Prisca.Quadroni@ai-lsc.ch

MAURO QUADRONI
Mlaw, Lawyer
Mauro.Quadroni@ai-lsc.ch

Swiss data protection

What’s in store for me, what do I have to do?

SWISS MEDTECH

healthcare projects
consulting & management Stein

Agenda

Dealing with customer and health data in the case of feedback from the market, complaints and vigilance.

Health data in medical devices - where is this data located and what must be observed during service, repair, maintenance, disposal? - Organizational measures

Health data in medical devices - What technical measures should be taken during product development and throughout the product life cycle?

SWISS MEDTECH

healthcare projects
consulting & management Stein

Feedback – Complaint - Vigilance

Privacy Policy

Reference to Regulation

MedDO, nDSG

EU MDR 2017/745, GSPR

SWISS MEDTECH

healthcare projects
consulting & management Stein

Feedback – Complaint - Vigilance

Awareness of what data are needed for the process.

Awareness of retention periods.

Awareness of who has access to data.

Awareness of organizational and technical protection measures.

Awareness of documentation.

Health data in medical devices

– Where are the data? – Why is this relevant?

Awareness of which products store data.

Products with internal memories e.g. HDD, SSD, …

What applies to products are picked up or sent for repair and maintenance from healthcare facilities?

What applies to products that are serviced on site?

What happens to the storage components during repair, maintenance, disposal? Who has access? How to protect?

SWISS MEDTECH

healthcare projects
consulting & management Stein

Health data in medical devices
– What about the processes?

In the focus: Processes / SOP`s - Employee training - Privacy policy

What are the **processes and documents** regarding workflows for

- Service
- Maintenance
- Repair on site
- Repair off site
- Replace of memories and devices
- Disposal of memories and devices

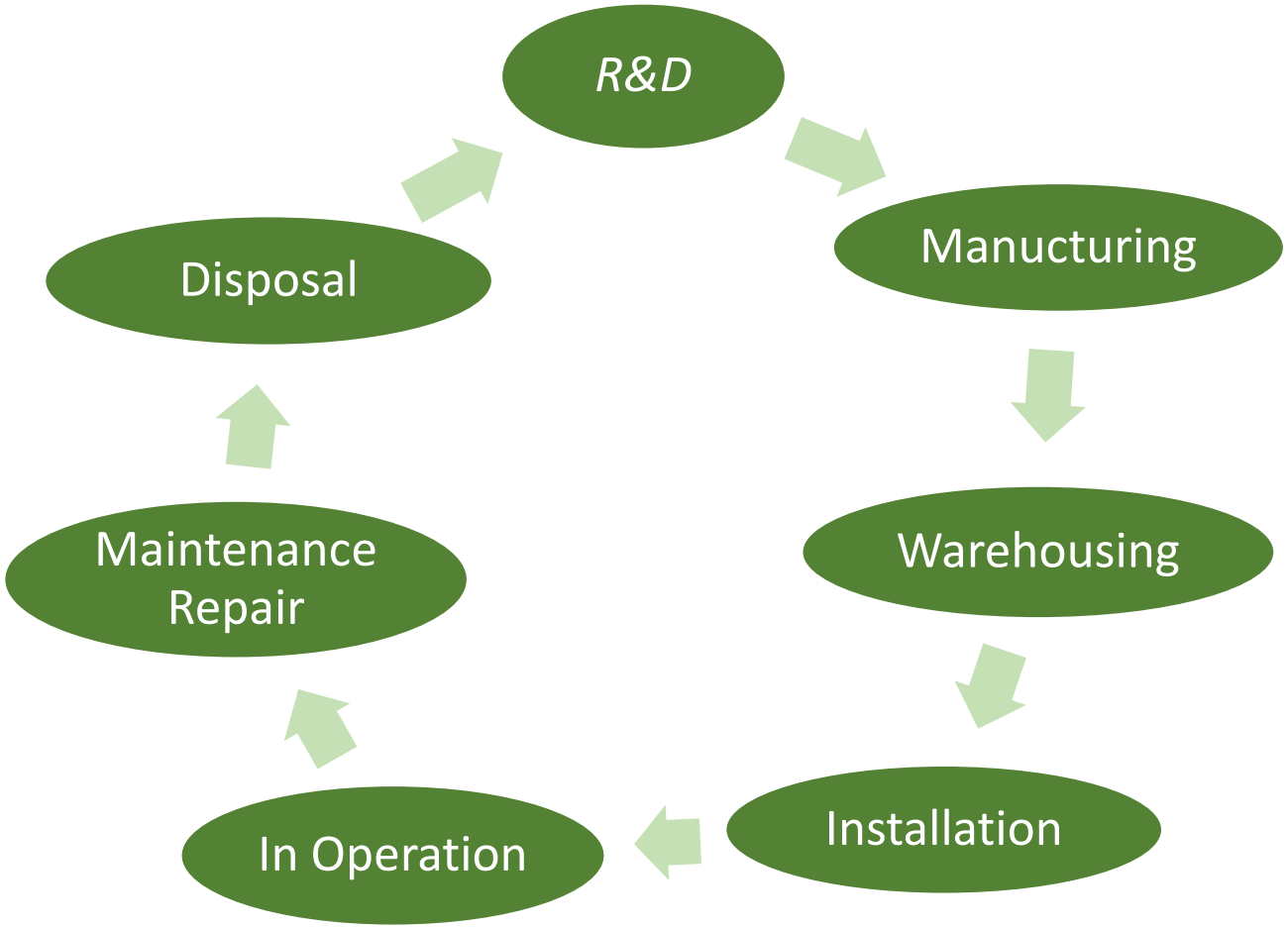
?

SWISS MEDTECH

healthcare projects
consulting & management Stein

Health data in medical devices

– What about technical measures in the product lifecycle?



SWISS MEDTECH

healthcare projects
consulting & management Stein

Health data in medical devices

– What about technical measures in the product lifecycle?

R&D

Functions to remove patient data finally

Cybersecurity functionality

Remote-maintenance functionality

Manufacturing

Function testing and documentation

SWISS MEDTECH

healthcare projects
consulting & management Stein

Health data in medical devices

– What about technical measures in the product lifecycle?

Warehousing / Delivery

Protection against unauthorized access to the product and data stored therein

Installation

Installation in the hospital IT environment

Training in data protection functions

SWISS MEDTECH

healthcare projects
consulting & management Stein

Health data in medical devices

– What about technical measures in the product lifecycle?

In Operation

Activated data protection and cybersecurity functions

Event logging

Maintenance / Repair / Disposal

Removal of patient data before removal / disposal of memory or transportation outside the healthcare facility

SWISS MEDTECH

healthcare projects
consulting & management Stein

Questions & Answers

SWISS MEDTECH

healthcare projects
consulting & management Stein