DPMF: A Modeling Framework for Data Protection by Design

Laurens Sion

17 November 2020, CIF Seminar

DistriNet

Joint work in context of PRiSE Project

PRiSE Project
Privacy-by-design Regulation in Software Engineering

Pierre Dewitte[+], Dimitri Van Landuyt[*], Kim Wuyts[*], Peggy Valcke[+], and Wouter Joosen[*]

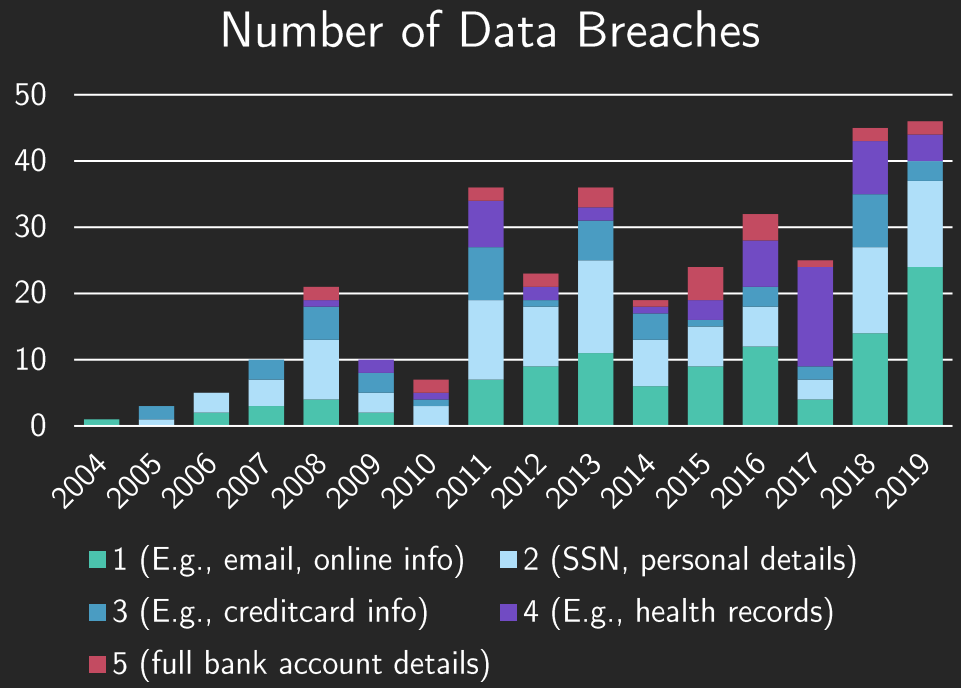
[*] imec-DistriNet, Dept. of Computer Science
[+] imec-CiTiP, Faculty of Law

Forces to Data Protection by Design

Pressure from incidents
Increasingly sensitive data breaches

Regulatory pressure
GDPR requiring appropriate measures

Forces to Data Protection by Design



Data: *Information is beautiful: World's Biggest Data Breaches*

Pressure from incidents

Increasingly sensitive data breaches

Regulatory pressure

GDPR requiring appropriate measures

Forces to Data Protection by Design

Art. 25 Data Protection by Design and by Default

"[...] the controller shall [...] implement appropriate technical and organisational measures [...] designed to implement data-protection principles [...]."

Pressure from incidents

Increasingly sensitive data breaches

Regulatory pressure

GDPR requiring appropriate measures

Data Protection by Design

Components of Data Protection by Design

5 components

Consider risk
to data subjects' rights and freedoms

Ensure compliance
with GDPR requirements

Implement measures
both technical and organizational

Demonstrate
accordance with the rules

When determining means processing
and during the processing itself

Data Protection Impact Assessment

to realize obligations DPbD

Mandatory when high risk

to data subjects' rights and freedoms

Groundwork for risk-based approach

to determine necessity DPIA

Existing approaches to DPIA

Templates, Questionnaires
Spreadsheets, documents, questionnaires to fill in

Extending software design models
Not all data protection concepts map to design model elements

Privacy and Security Requirements Engineering
Limited coverage of data protection concepts

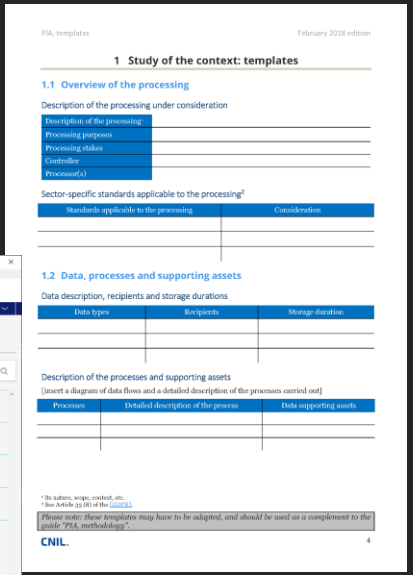
Existing approaches to DPIA

Templates, Questionnaires
Spreadsheets, documents, questionnaires to fill in

Extending design models
Not all data protection concepts map to design model elements

Privacy and Security RE
Limited coverage of data protection concepts

Existing approaches to DPIA



Templates, Questionnaires

Spreadsheets, documents, questionnaires to fill in

Extending design models

Not all data protection concepts map to design model elements

Privacy and Security RE

Limited coverage of data protection concepts

Existing approaches to DPIA

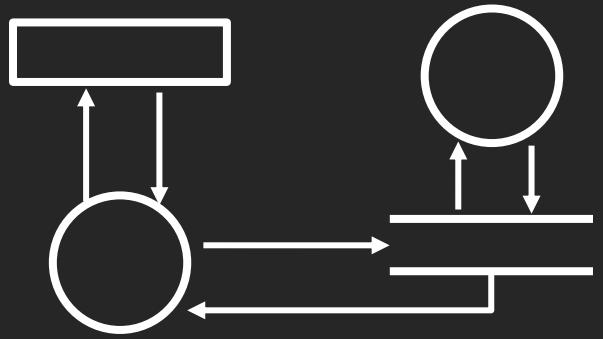
The organization controlling the processing is not present in the software design model

Templates, Questionnaires
Spreadsheets, documents, questionnaires to fill in

Extending design models
Not all data protection concepts map to design model elements

Privacy and Security RE
Limited coverage of data protection concepts

Existing approaches to DPIA



Are there automated decisions on special categories of personal data?

Templates, Questionnaires
Spreadsheets, documents, questionnaires to fill in

Extending design models
Not all data protection concepts map to design model elements

Privacy and Security RE
Limited coverage of data protection concepts

Our Approach to Data Protection by Design

Different Stakeholders use Different Models & Views

Software Engineers

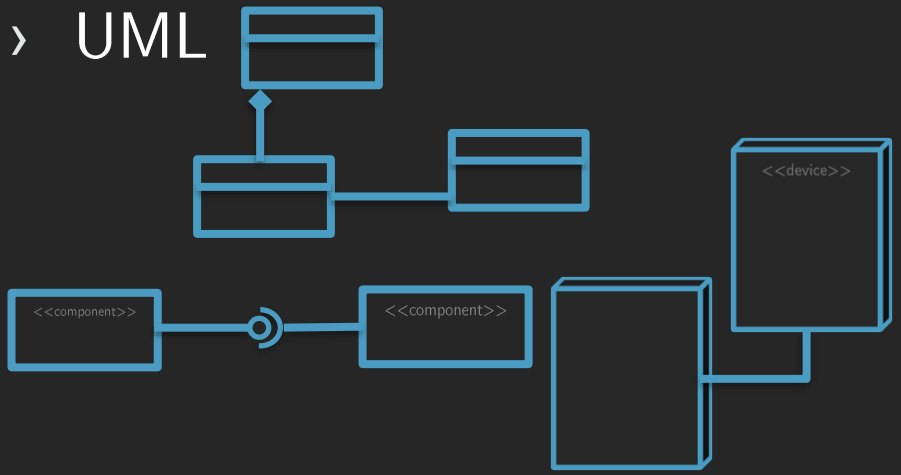
Legal Stakeholders

Different Stakeholders use Different Models & Views

Software Engineers

Legal Stakeholders

- UML

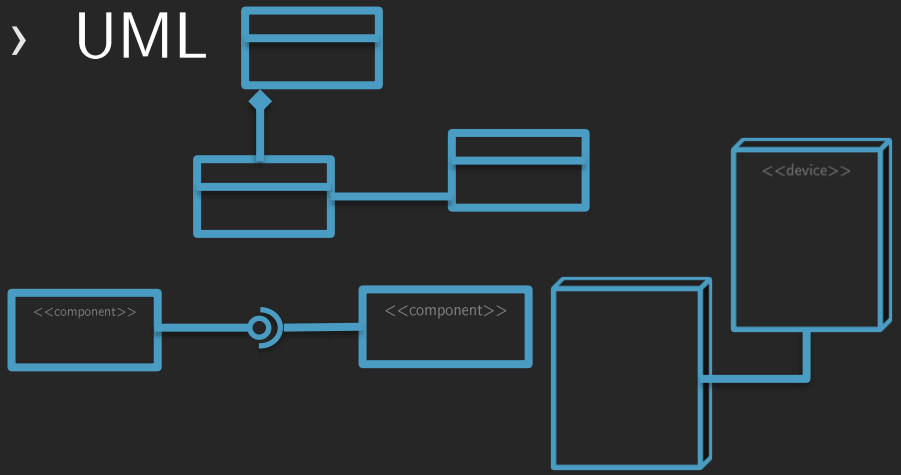


Different Stakeholders use Different Models & Views

Software Engineers

Legal Stakeholders

- UML

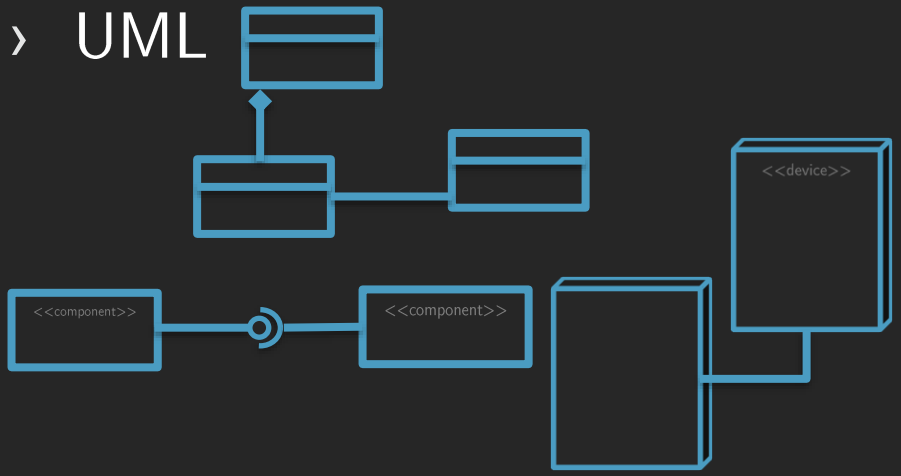


- Threat Modeling

Different Stakeholders use Different Models & Views

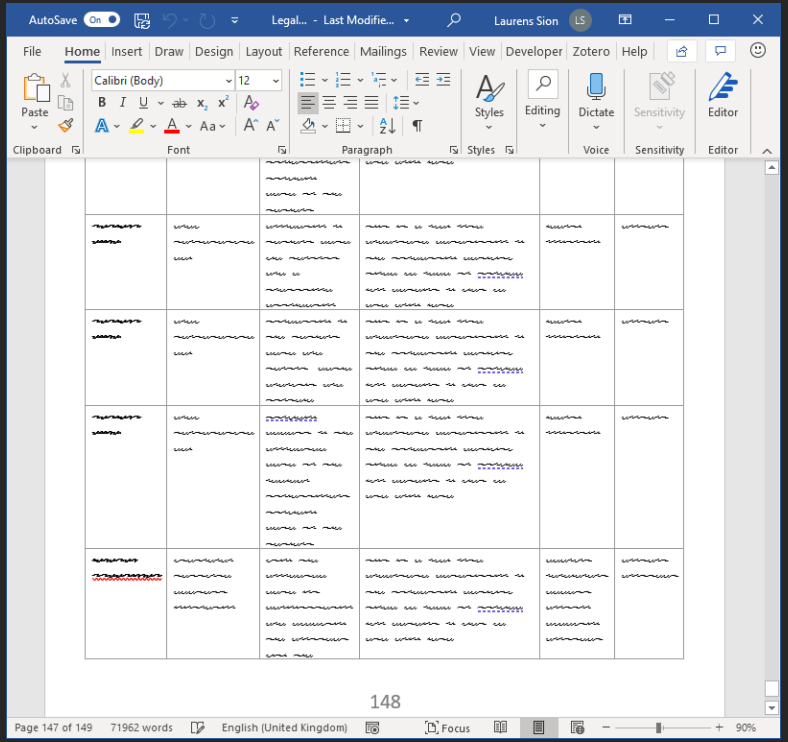
Software Engineers

- UML



- Threat Modeling

Legal Stakeholders



Interdisciplinary approach

Software Engineers

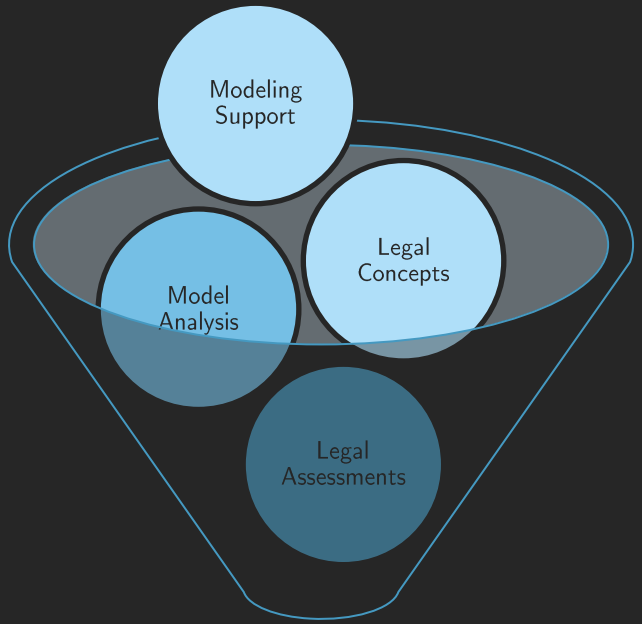
Modeling support
to capture processing operations

Model queries and analysis
to identify problems

Legal Stakeholders

Concepts
processing, rationale, ...

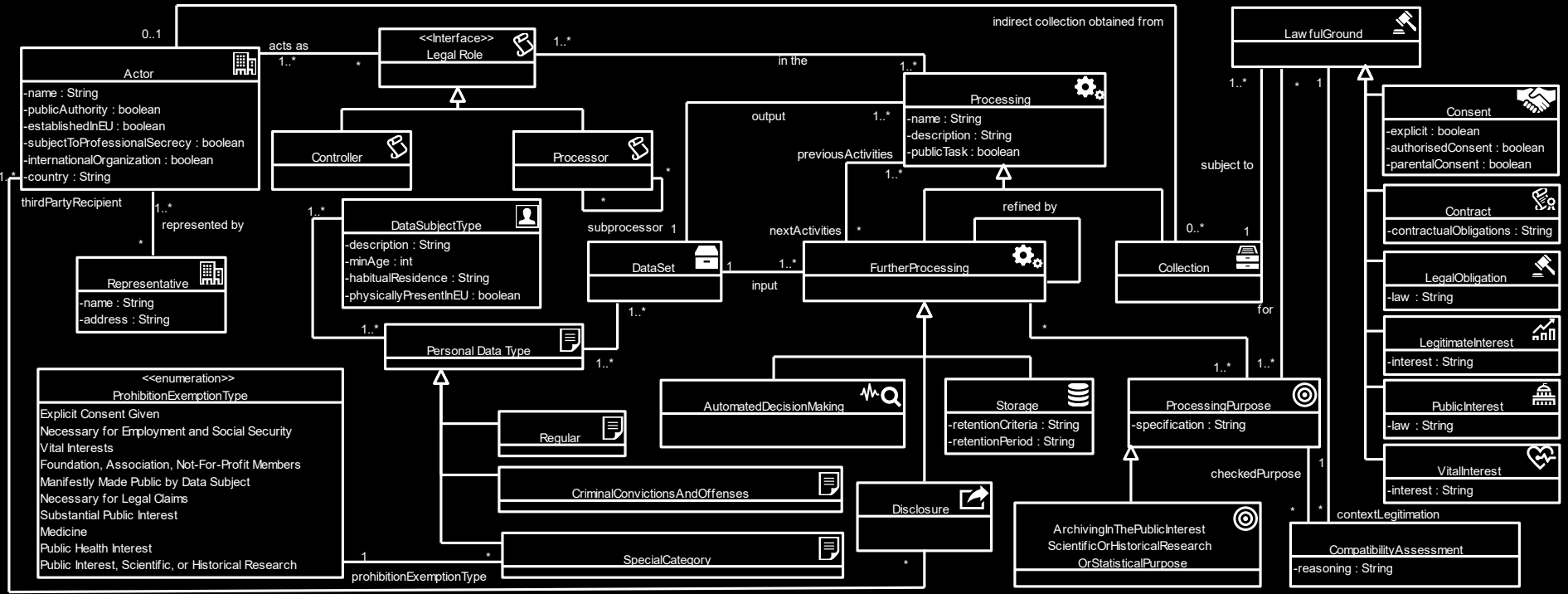
Legal assessments
for compliance


Modeling
Support
Legal
Concepts
Model
Analysis
Legal
Assessments

Key Components Approach

1. Structured modeling
   Key concepts
2. Automated sanity checks
   Completeness
3. Tool-supported legal assessments
   Embed legal argumentation
4. Automated generation of outputs
   Documentation

1. Structured modeling


Actor
-name : String
-publicAuthority : boolean
-establishedInEU : boolean
-subjectToProfessionalSecrecy : boolean
-internationalOrganization : boolean
-country : String
<<Interface>>
Legal Role
acts as
Controller
Processor
Representative
-name : String
-address : String
thirdPartyRecipient
represented by
DataSubjectType
-description : String
-minAge : int
-habitualResidence : String
-physicallyPresentInEU : boolean
Personal Data Type
DataSet
subprocessor
input
output
Processing
-name : String
-description : String
-publicTask : boolean
previousActivities
nextActivities
FurtherProcessing
refined by
in the
indirect collection obtained from
Collection
for
subject to
LawfulGround
Consent
-explicit : boolean
-authorisedConsent : boolean
-parentalConsent : boolean
Contract
-contractualObligations : String
LegalObligation
-law : String
LegitimateInterest
-interest : String
PublicInterest
-law : String
VitalInterest
-interest : String
contextLegitimation
CompatibilityAssessment
-reasoning : String
ProcessingPurpose
-specification : String
checkedPurpose
ArchivingInThePublicInterest
ScientificOrHistoricalResearch
OrStatisticalPurpose
Storage
-retentionCriteria : String
-retentionPeriod : String
AutomatedDecisionMaking
Disclosure
Regular
CriminalConvictionsAndOffenses
SpecialCategory
<<enumeration>>
ProhibitionExemptionType
Explicit Consent Given
Necessary for Employment and Social Security
Vital Interests
Foundation, Association, Not-For-Profit Members
Manifestly Made Public by Data Subject
Necessary for Legal Claims
Substantial Public Interest
Medicine
Public Health Interest
Public Interest, Scientific, or Historical Research
prohibitionExemptionType

Four categories of concepts

Actors and their roles
Organization, controller, ...

Processing activities
Collection, disclosure, ...

Data types and subjects
Data subject type, data type, ...

Legal rationale
Purpose, Lawful grounds, ...

Four categories of concepts


Actor


Representative


Controller


Processor

Actors and their roles
Organization, controller, ...

Processing activities
Collection, disclosure, ...

Data types and subjects
Data subject type, data type, ...

Legal rationale
Purpose, Lawful grounds, ...

Four categories of concepts

Actors and their roles
Organization, controller, ...

Processing activities
Collection, disclosure, ...

Data types and subjects
Data subject type, data type, ...

Legal rationale
Purpose, Lawful grounds, ...

Four categories of concepts

DataSubject Type

DataSet

Personal DataType

Actors and their roles
Organization, controller, ...

Processing activities
Collection, disclosure, ...

Data types and subjects
Data subject type, data type, ...

Legal rationale
Purpose, Lawful grounds, ...

Four categories of concepts

Actors and their roles
Organization, controller, ...

Processing activities
Collection, disclosure, ...

Data types and subjects
Data subject type, data type, ...

Legal rationale
Purpose, Lawful grounds, ...

2. Automated sanity checks

Meta-model imposes rules

Some examples...

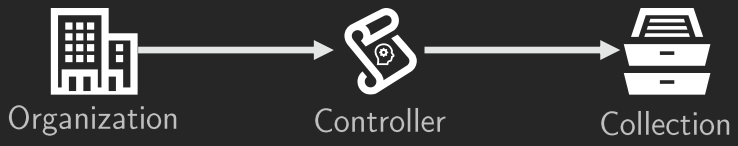
Actors' involvement in processing
E.g., organization as controller

Further processing follows collection
Chain of processing operations

Further processing must have purpose
To enable compatibility assessment

Meta-model imposes rules

Some examples...



Actors' involvement in processing

E.g., organization as controller

Further processing follows collection

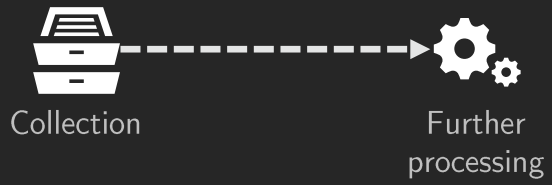
Chain of processing operations

Further processing must have purpose

To enable compatibility assessment

Meta-model imposes rules

Some examples...



Actors' involvement in processing
E.g., organization as controller

Further processing follows collection
Chain of processing operations

Further processing must have purpose
To enable compatibility assessment

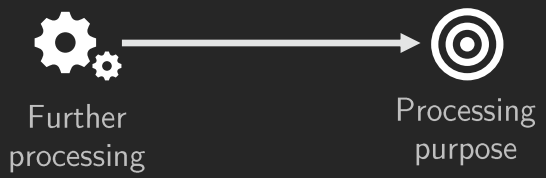
Meta-model imposes rules

Some examples...

Actors' involvement in processing
E.g., organization as controller

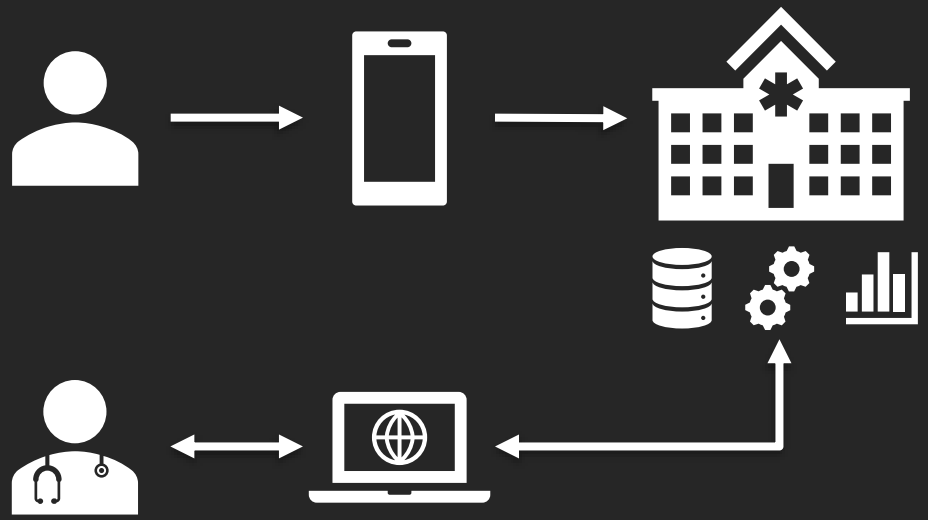
Further processing follows collection
Chain of processing operations

Further processing must have purpose
To enable compatibility assessment



3. Tool-supported legal assessments

Illustration: Patient Monitoring System



Patient Monitoring System

Patient Monitoring System

Soundness Check

Does every further processing link back to original collection?

Patient Monitoring System

Soundness Check

Does every further processing link back to original collection?

Patient Monitoring System

Soundness Check

Does every further processing link back to original collection?

Is there a controller for every processing activity?

Patient Monitoring System

Soundness Check

Does every further processing link back to original collection?

Is there a controller for every processing activity?

Patient Monitoring System

Soundness Check

Does every further processing link back to original collection?

Is there a controller for every processing activity?

Patient Monitoring System

PMS Company

GP

Patient Data Collection

Health Risk Assessment

Storage and Archival

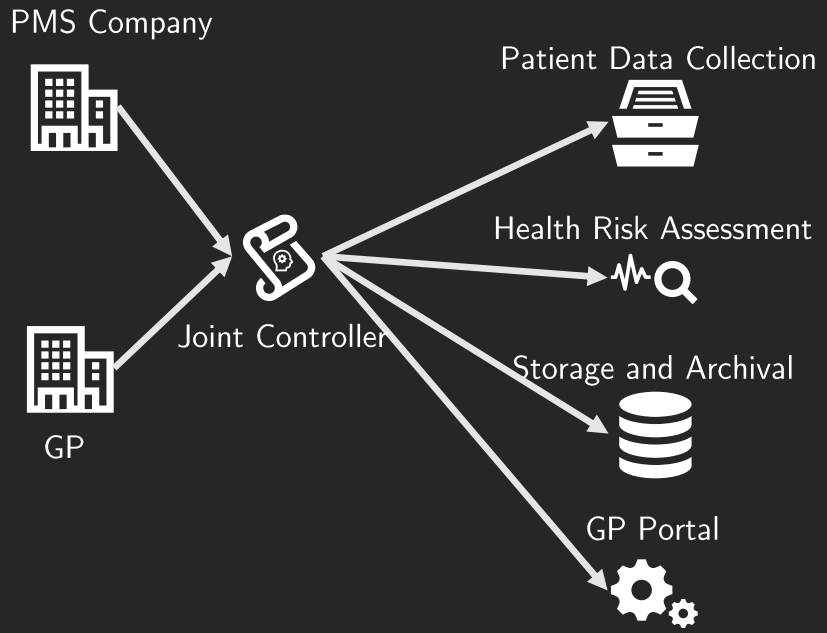
GP Portal

Soundness Check

Does every further processing link back to original collection?

Is there a controller for every processing activity?

Patient Monitoring System

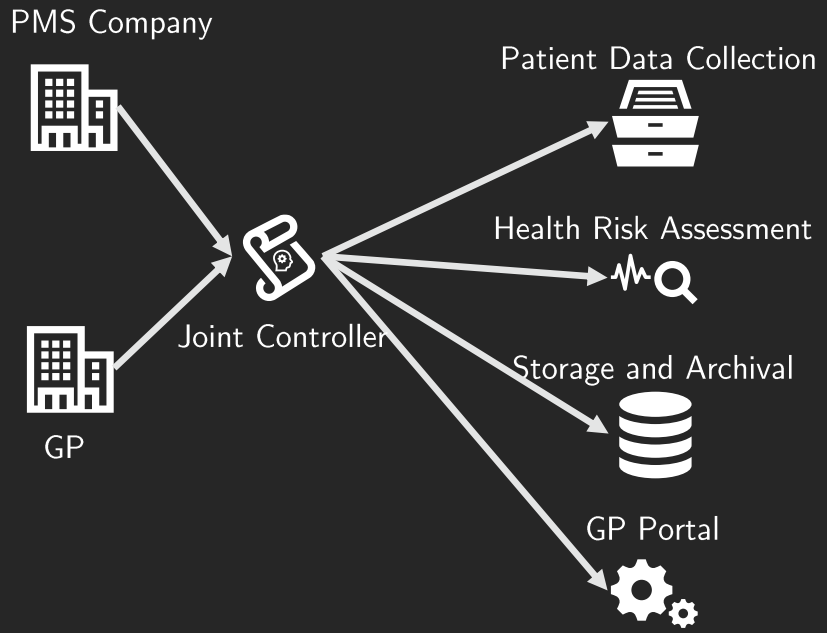


Soundness Check

Does every further processing link back to original collection?

Is there a controller for every processing activity?

Patient Monitoring System

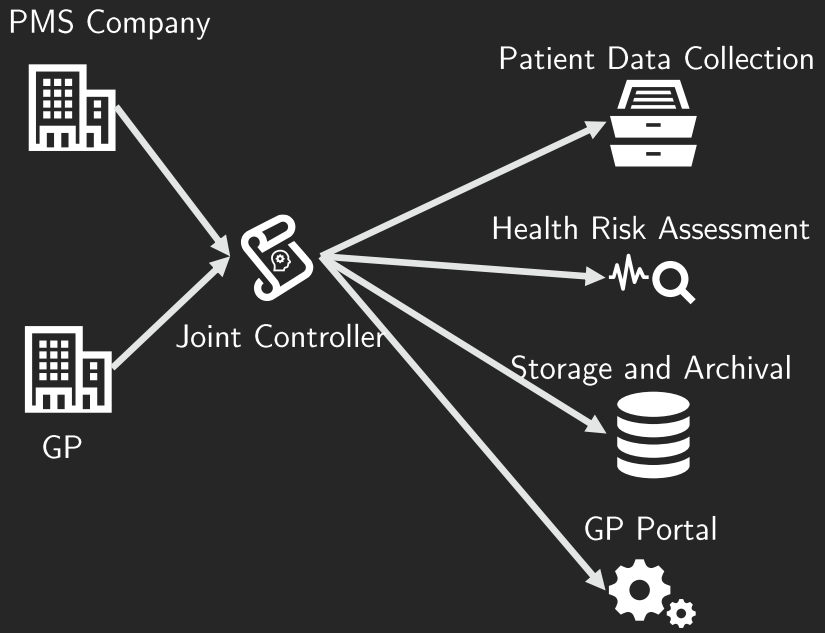


Soundness Check

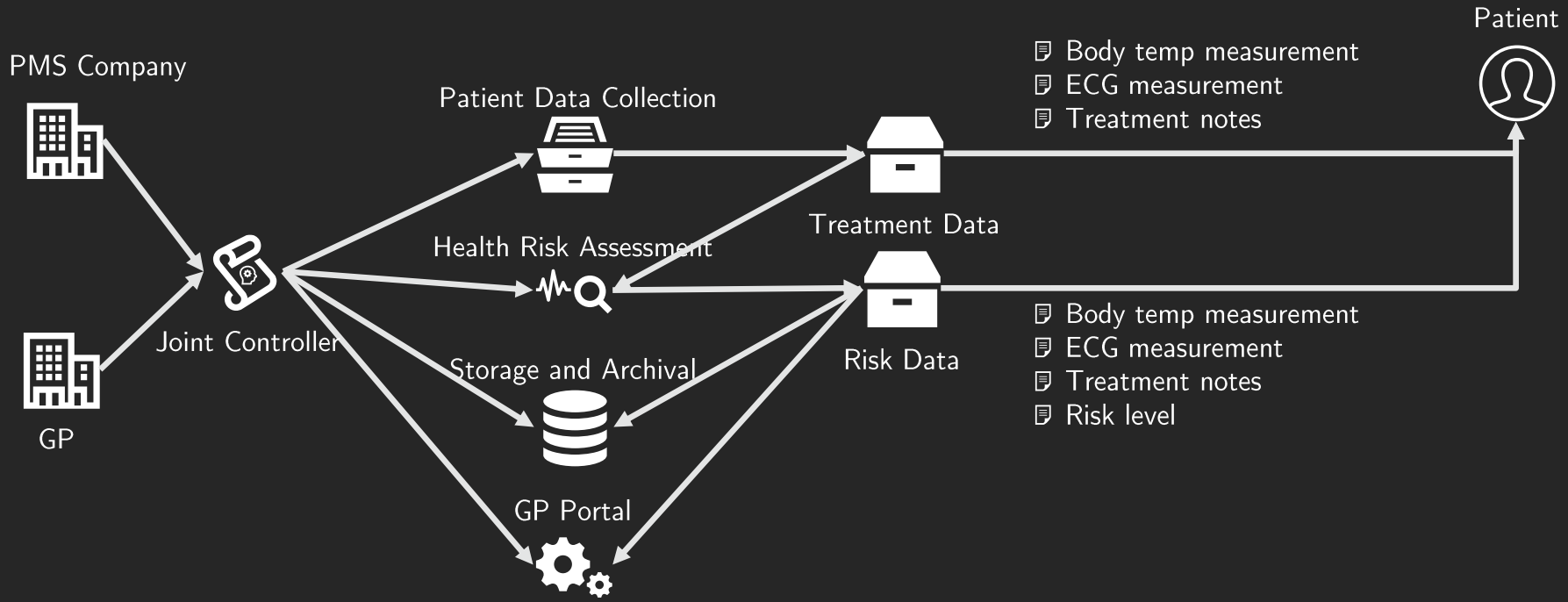
Does every further processing link back to original collection?

Is there a controller for every processing activity?

Patient Monitoring System



Patient Monitoring System



Patient Monitoring System

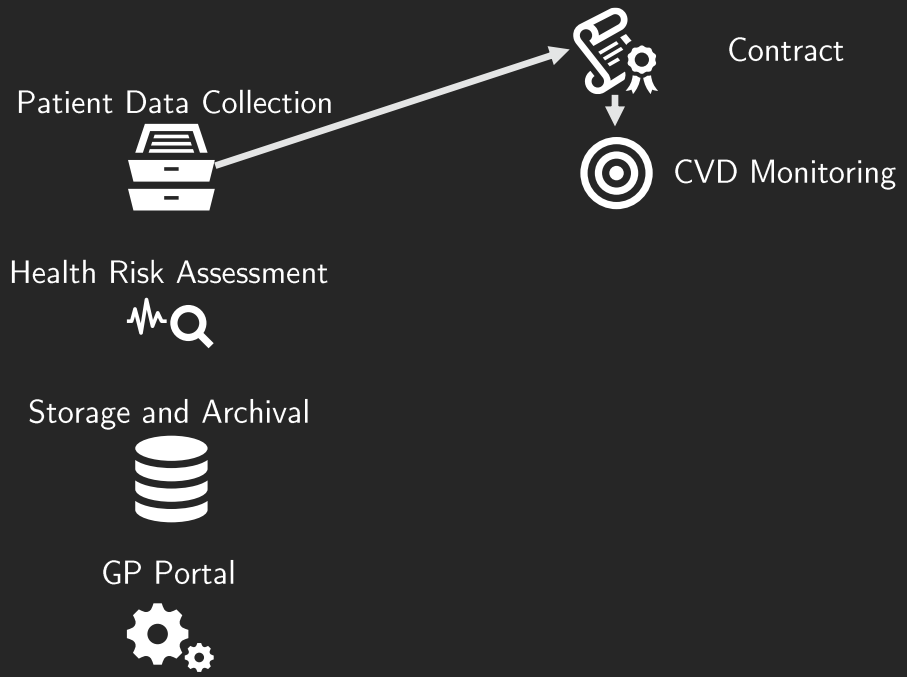
Patient Data Collection

Health Risk Assessment

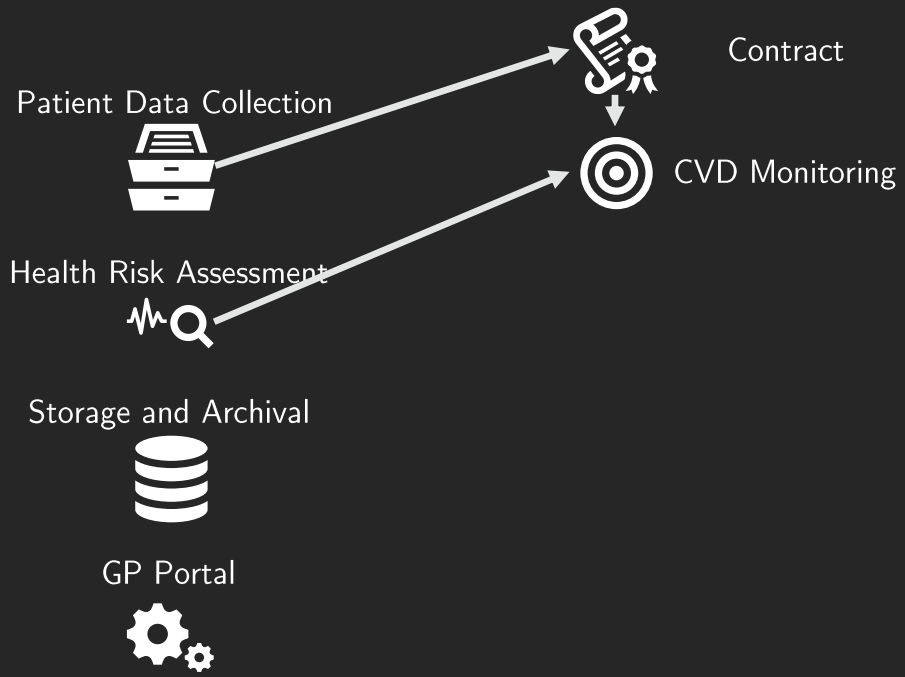
Storage and Archival

GP Portal

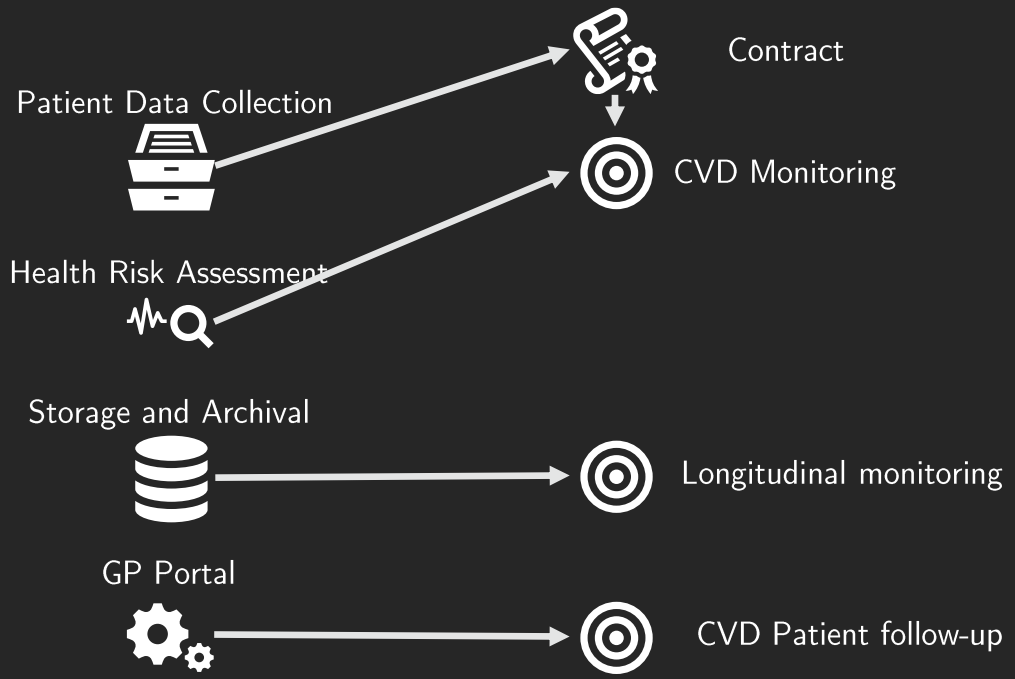
Patient Monitoring System



Patient Monitoring System

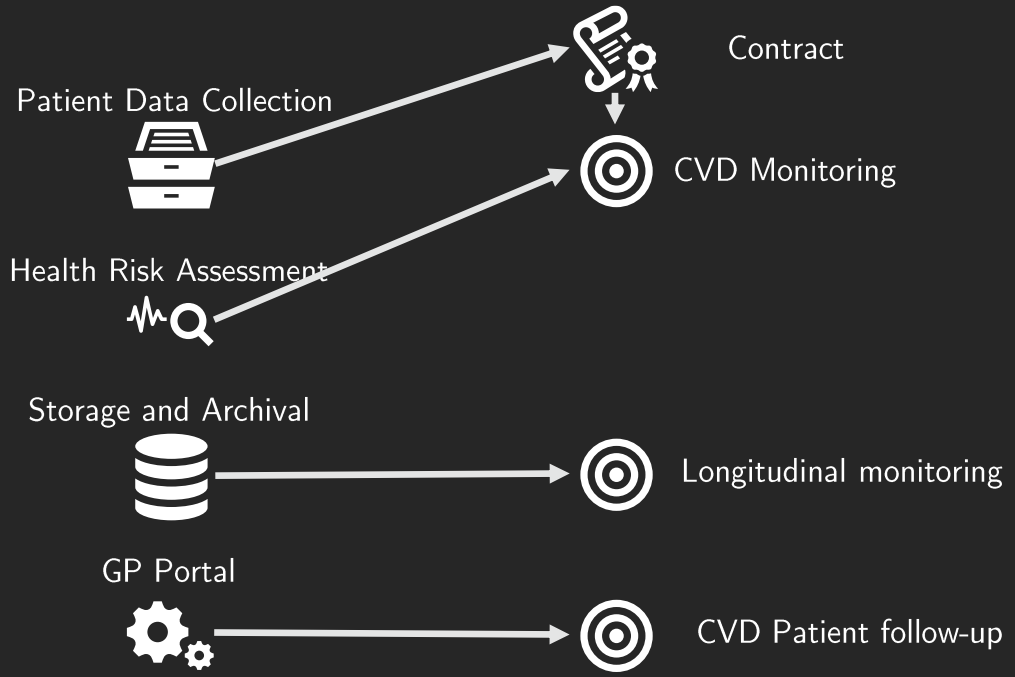


Patient Monitoring System

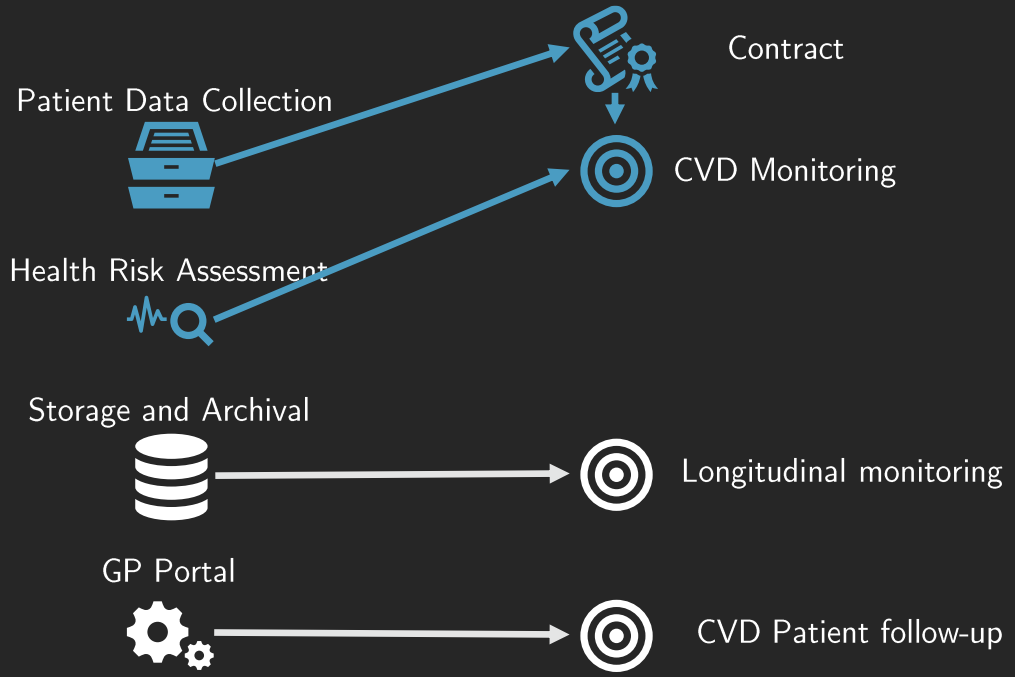


Patient Monitoring System

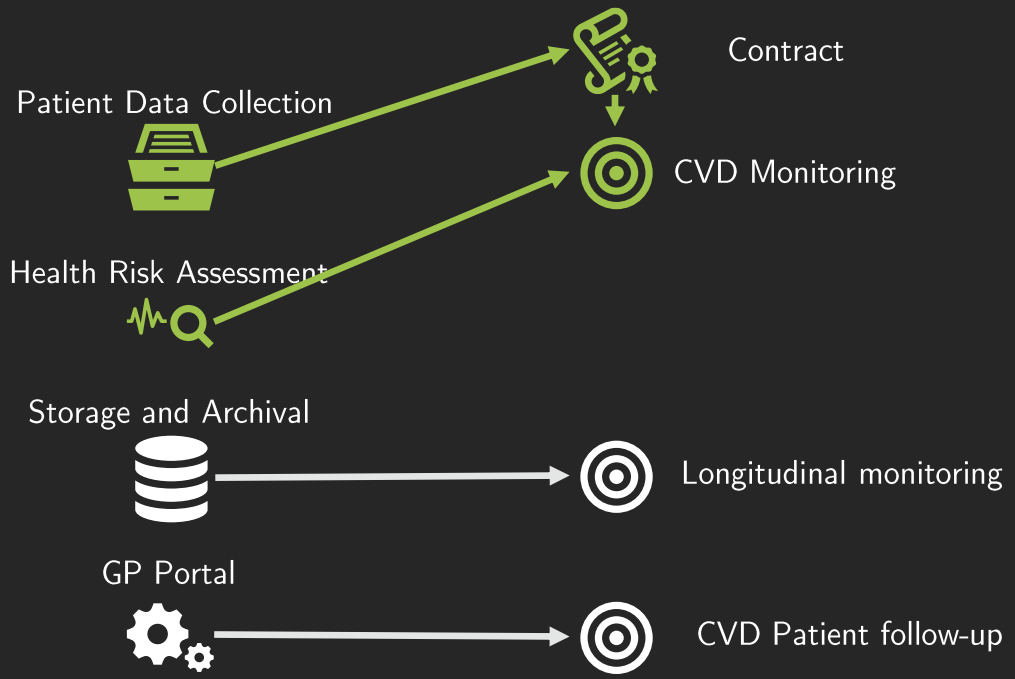
Compatibility Assessment



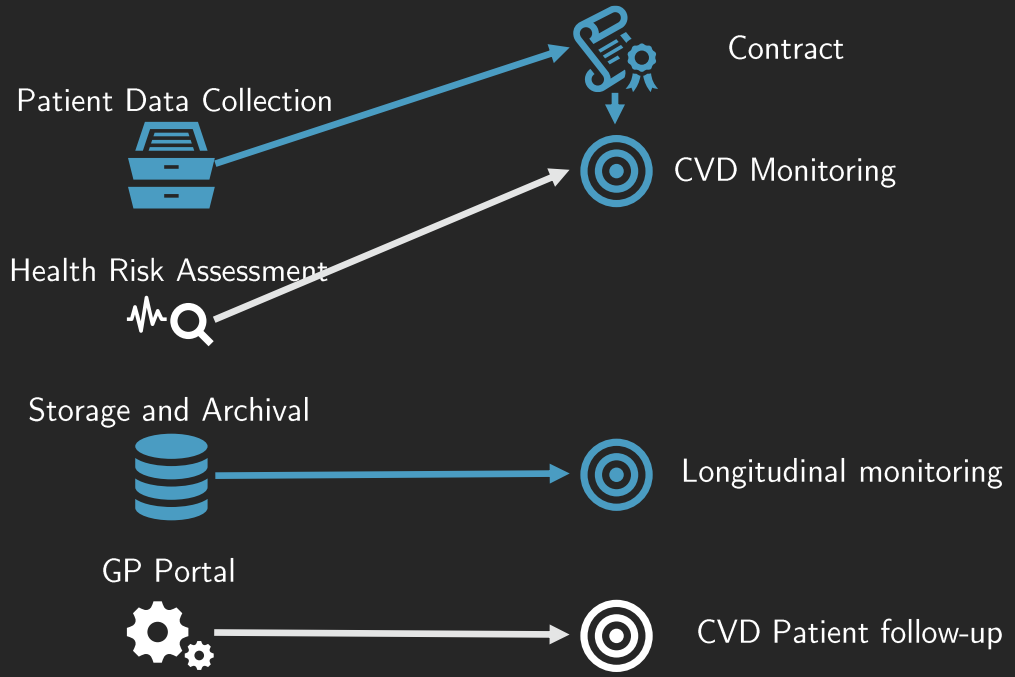
Patient Monitoring System



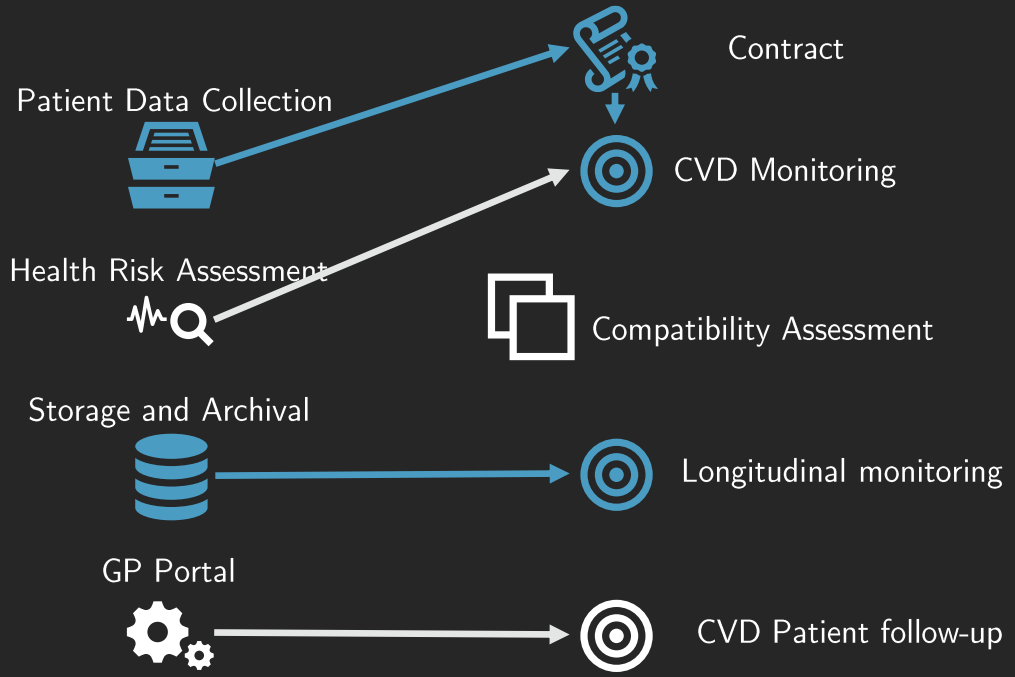
Patient Monitoring System



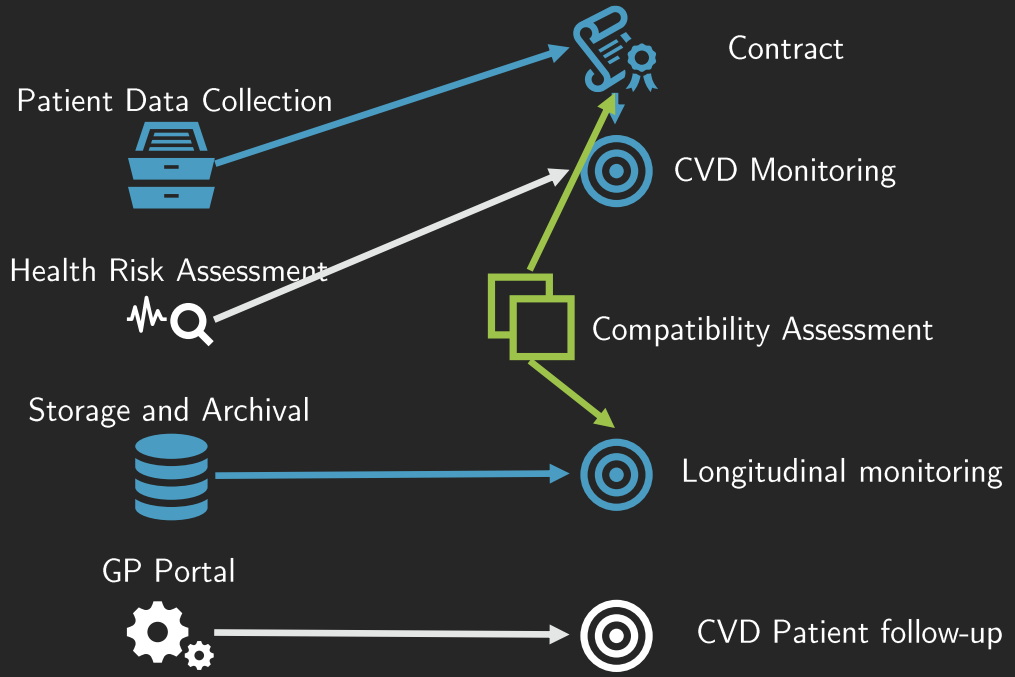
Patient Monitoring System



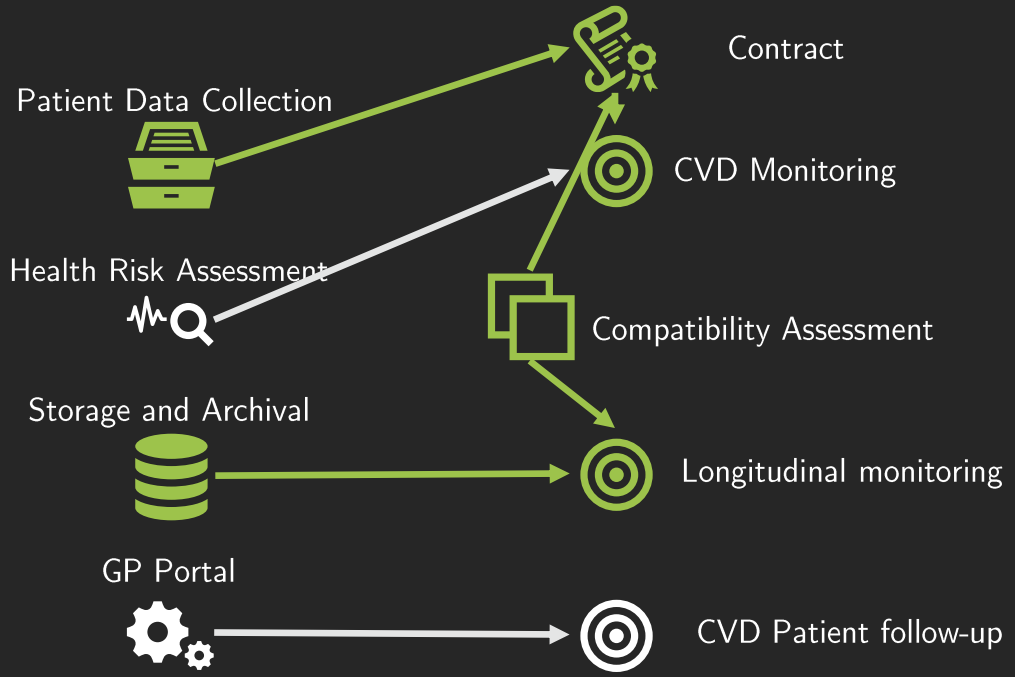
Patient Monitoring System



Patient Monitoring System



Patient Monitoring System



In-depth Scenario-based Validation

Applied on eHealth System

Patient Monitoring System for patients with cardiovascular diseases

Scenarios:

- Construction and analysis of initial description
- Extension for emergency services notification
- Further use for scientific research

Every change triggers full re-assessment

Ensure that modifications do not introduce new problems

Support Analysis

Avoid obvious problems

E.g., missing EU representative

Assist in compliance assessment

Ensure systematic analysis of all processing operations

4. Automated generation of outputs

Not only analysis, also documentation

Supervisory Authorities
Documentation to demonstrate compliance

Data Subjects
For every data subject: processed data and purposes

Privacy Policies
Support writing policy using information from model

Tool support

Model creation
Sanity checks on processing operations

(Semi-)Automated Assessments
Guide legal assessments

Export documentation
Extract relevant information from model

Tool support

Eclipse-based product

Eclipse Modeling Framework, Sirius,

Model queries in VIATRA

- to perform the legal assessments
- to extract relevant information for documentation export

Demo

Future work

Supporting mitigations
How to capture legal mitigations in the models?

In-depth comparative evaluation with existing DPIAs
E.g., DPIAs on contact tracing apps

Risk analysis
Quantifying legal risk, prioritizing legal compliance problems

Model-based compliance assessment provides compelling benefits

Single central source of information
Avoid duplicated and inconsistent information

Combine processing activities with compliance results
Documented by design in the same model

Ensure previous assessment remain accurate
Evaluate whether changes invalidate previous assessments

Realizing Data Protection by Design with Interdisciplinary Approach

Require both technical and legal expertise
Meet GDPR obligations, ensure appropriate measures

Leverage legal expertise
Comprehensive description, legal assessments, DPIA, ...

Leverage software engineering expertise
Models of data processing operations, automated sanity checking and analysis, ...

Thank you!

https://distrinet.cs.kuleuven.be/

Contact

DPMF: A Modeling Framework for Data Protection by Design
https://lirias.kuleuven.be/3264553

Website of the Data Protection Modeling Framework
https://distrinet.cs.kuleuven.be/software/dpmf/

Laurens Sion, Pierre Dewitte, Dimitri Van Landuyt, Kim Wuyts, Peggy Valcke, and Wouter Joosen
firstname.lastname@kuleuven.be

DPMF: A Modeling Framework for Data Protection by Design

Laurens Sion

17 November 2020, CIF Seminar

DistriNet