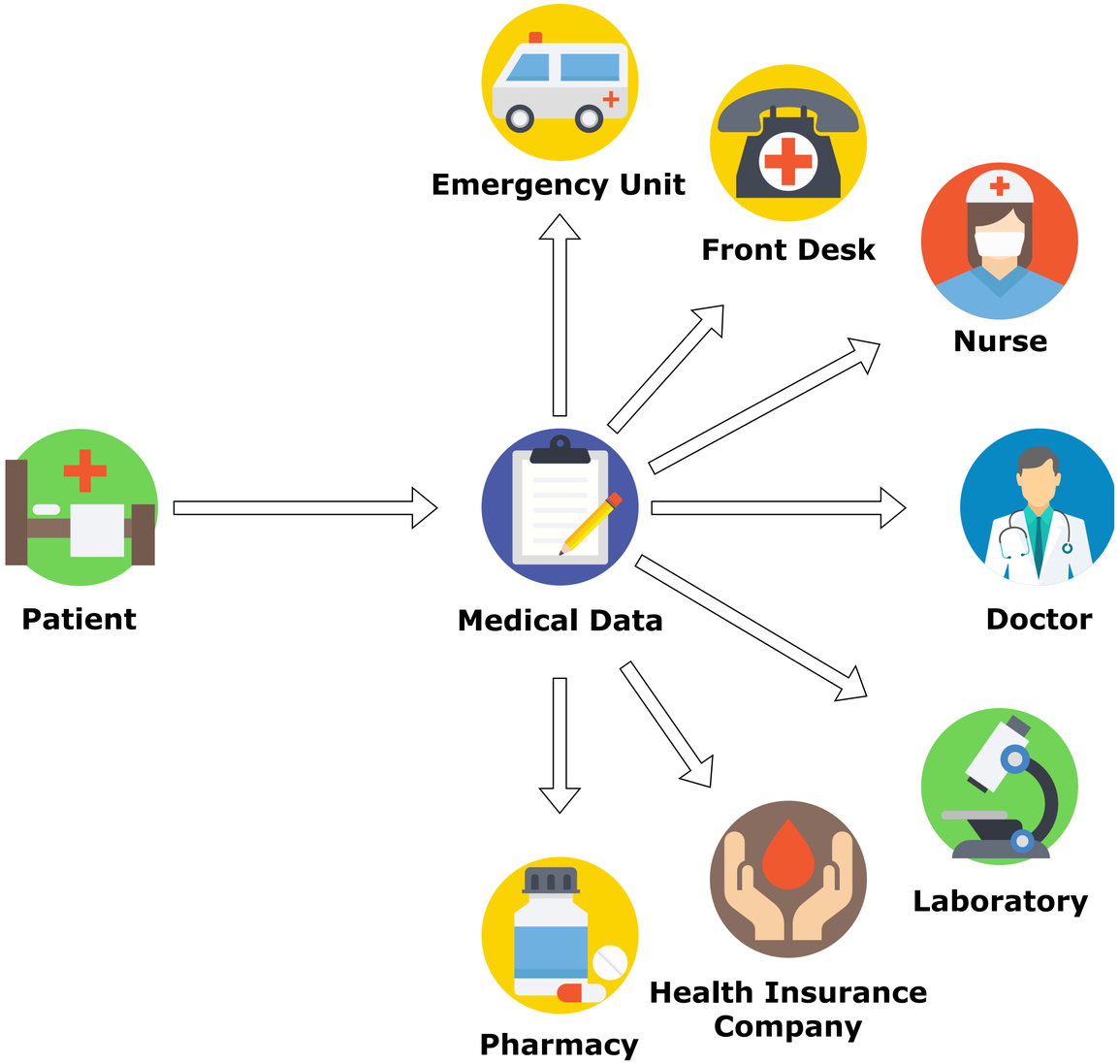
BUILDING PRIVACY AWARENESS INTO (CLINICAL) WORKFLOWS

S. Irem BESIK

besiksal @ informatik.hu-berlin.de

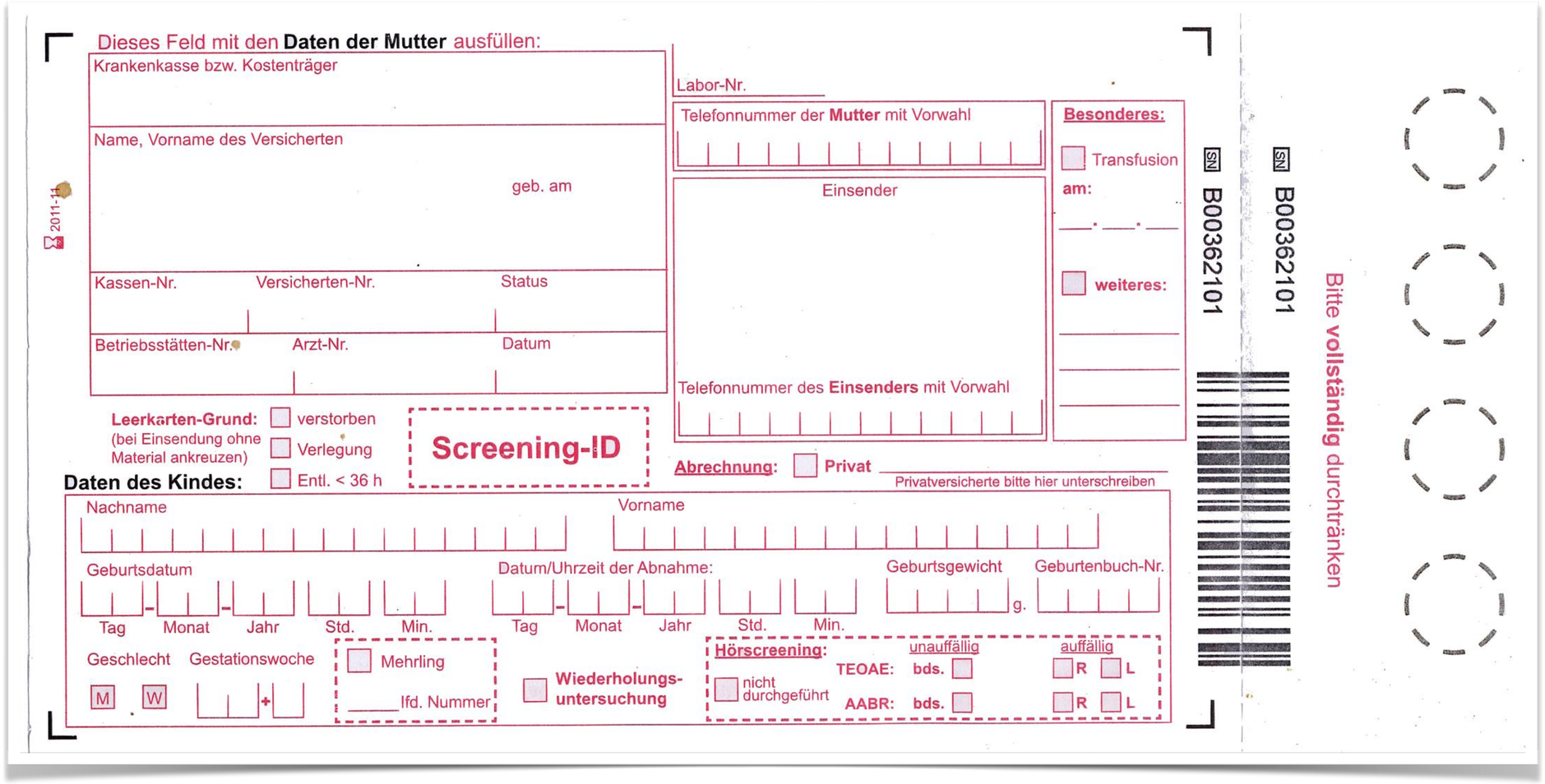
Supervisor: *Prof. Johann-Christoph Freytag, Ph.D.*

MOTIVATION: PRIVACY IN CLINICAL DOMAIN



- patients' personal medical data
- different healthcare providers

MOTIVATING EXAMPLE: NEWBORN SCREENING



MOTIVATING EXAMPLE: NEWBORN SCREENING

Desk

Pediatrician

Lab

demographic data

sensitive blood data

medical data

Dieses Feld mit den **Daten der Mutter** ausfüllen:

Krankenkasse bzw. Kostenträger

Name, Vorname des Versicherten

geb. am

Kassen-Nr. Versicherten-Nr. Status

Betriebsstätten-Nr. Arzt-Nr. Datum

Labor-Nr.

Telefonnummer der **Mutter** mit Vorwahl

Einsender

Telefonnummer des **Einsenders** mit Vorwahl

Besonderes:

Transfusion am: ___.___.___

weiteres:

Leerkarten-Grund: (bei Einsendung ohne Material ankreuzen) verstorben, Verlegung, Entl. < 36 h

Screening-ID

Abrechnung: Privat

Privatversicherte bitte hier unterschreiben

Daten des Kindes:

Nachname

Vorname

Geburtsdatum Tag Monat Jahr Std. Min.

Datum/Uhrzeit der Abnahme: Tag Monat Jahr Std. Min.

Geburtsgewicht g.

Geburtenbuch-Nr.

Geschlecht M W

Gestationswoche

Mehrling

lfd. Nummer

Wiederholungs-untersuchung

Hörscreening: nicht durchgeführt

	unauffällig	auffällig
TEOAE:	bds.	R L
AABR:	bds.	R L

SN B00362101

SN B00362101

Bitte **vollständig** durchtränken

PRIVACY BY DESIGN VIA CLINICAL WORKFLOWS

Clinical Workflow includes

a series of tasks for clinical services

also how tasks are performed, in what order, and by whom

RESEARCH PROBLEM

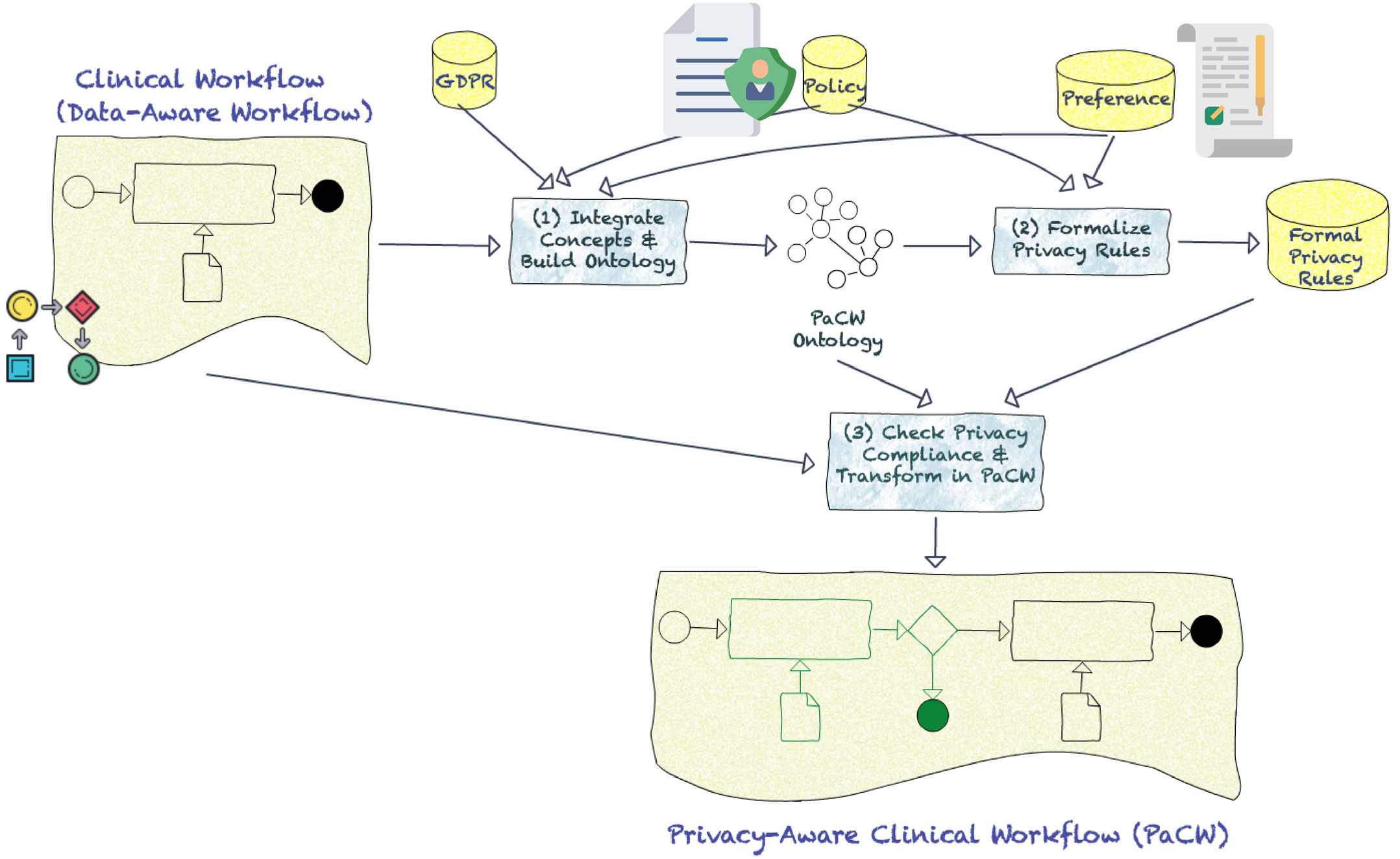
- Transforming non-privacy-aware clinical WFs into privacy-aware ones

- Privacy-aware WF is compliant with:

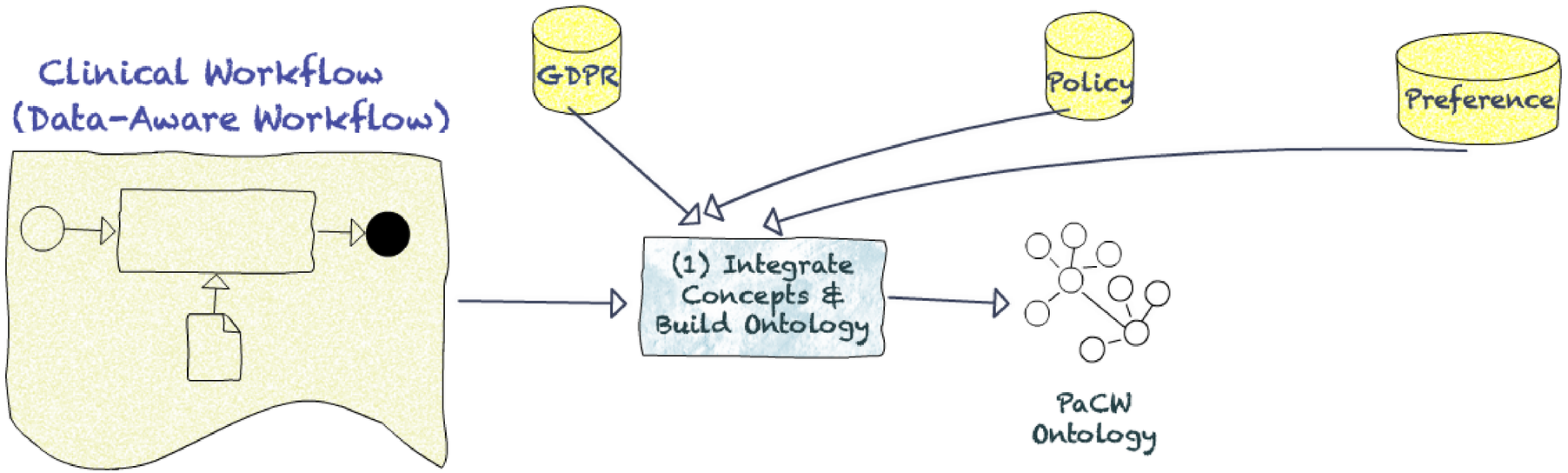
  1. privacy principles based on the EU General Data Protection Regulation (GDPR)

  2. privacy policies by healthcare providers

  3. privacy preferences of data subjects (patients)


Clinical Workflow
(Data-Aware Workflow)
GDPR
Policy
Preference
(1) Integrate Concepts & Build Ontology
PaCW Ontology
(2) Formalize Privacy Rules
Formal Privacy Rules
(3) Check Privacy Compliance & Transform in PaCW
Privacy-Aware Clinical Workflow (PaCW)

(1) INTEGRATE CONCEPTS



semantically represent privacy concepts and BPMN-based clinical workflows

↓

Privacy-**a**ware **C**linical **W**orkflow (PaCW) Ontology

PRIVACY PRINCIPLES BASED ON GDPR

GDPR, Europe's Data Privacy Law, Is So Long and Boring It Could 'Sedate a Buffalo'

By Sissi Cao • 06/04/18 2:02pm

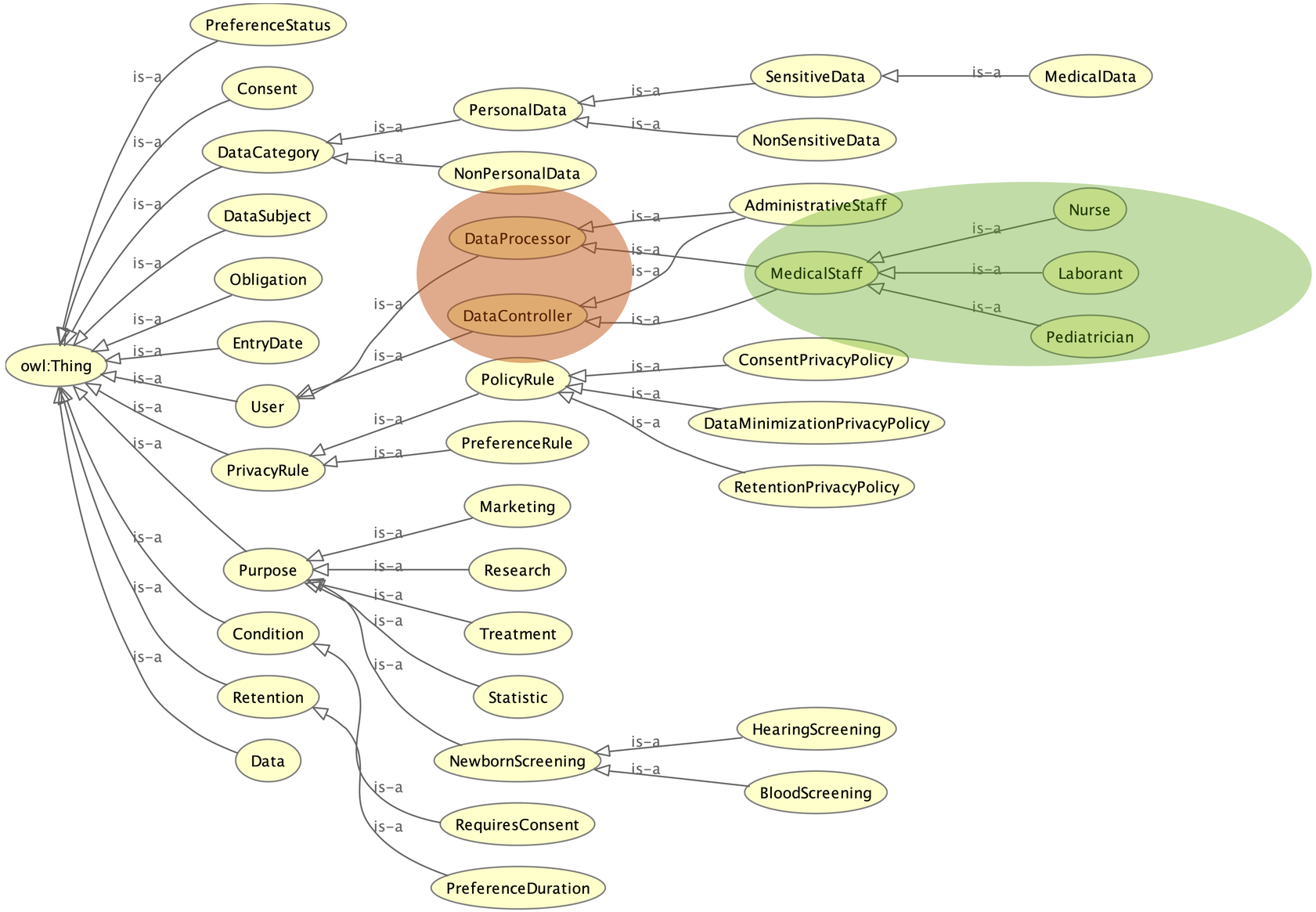
A BBC announcer-narrated GDPR will cure your insomnia in minutes. JEWEL SAMAD/AFP/Getty Images

PRIVACY PRINCIPLES BASED ON GDPR

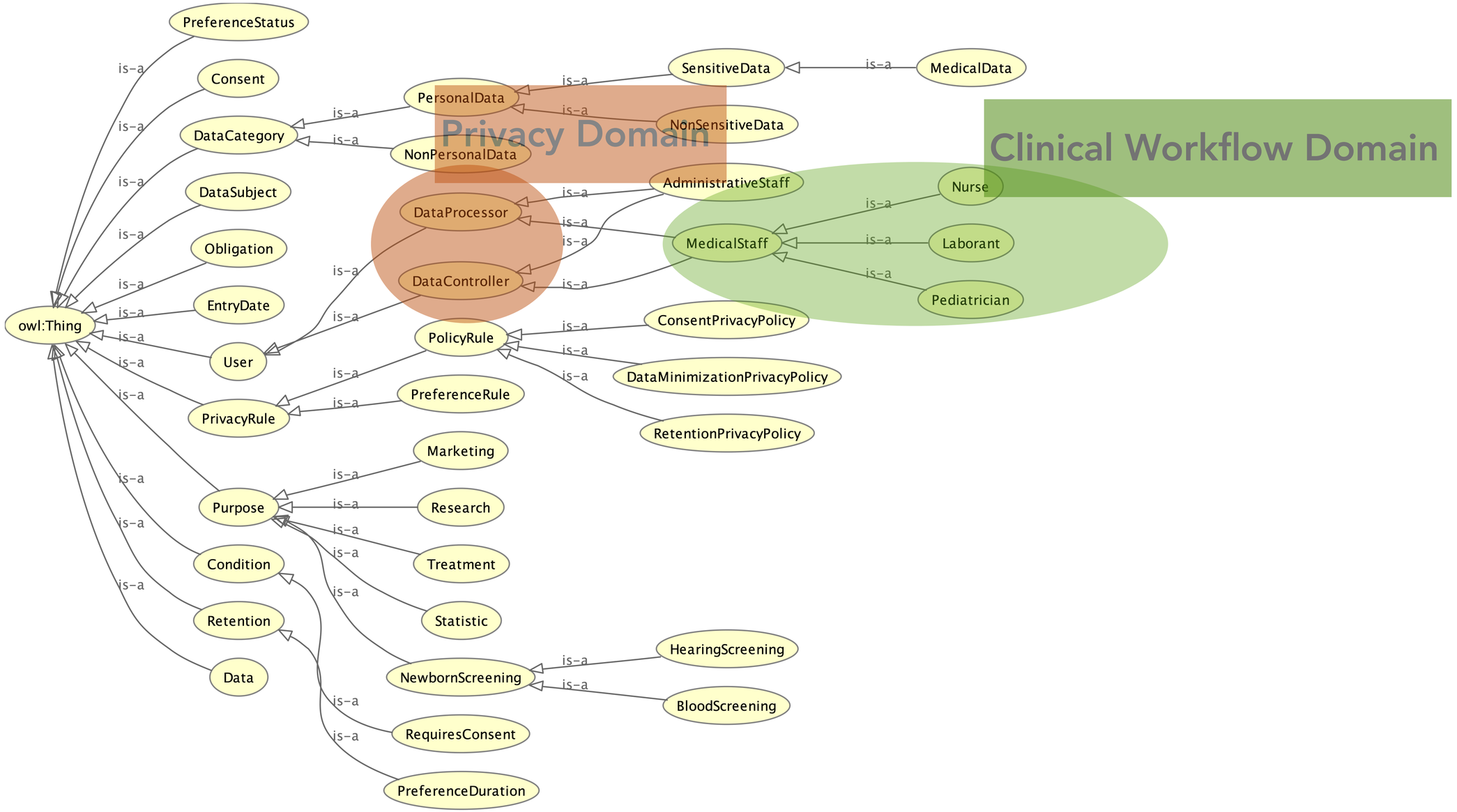
- Purpose Specification: Personal data be collected for specified purposes
- Consent Check: Data processing is lawful with an explicit consent of a data subject. *(e.g. optional procedures like newborn screening)*
- Limited Retention Period: Personal data be kept for no longer than is necessary
- Data Minimization: Personal data be limited to what is necessary

Privacy-aware Clinical Workflow (PaCW) Ontology

Privacy-aware Clinical Workflow (PaCW) Ontology

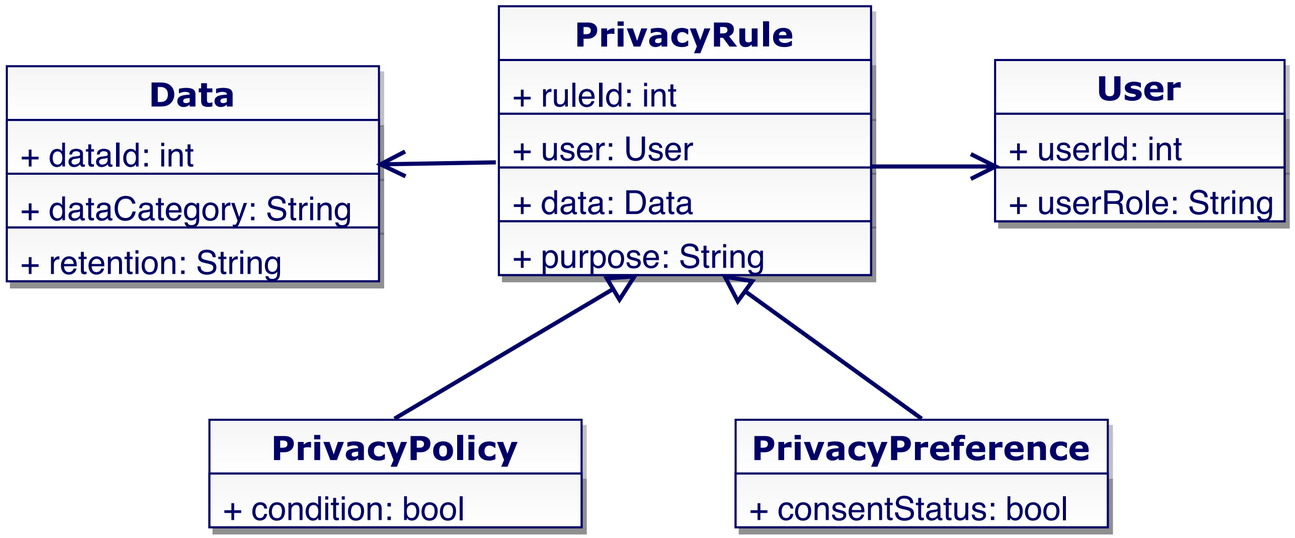


Privacy-aware Clinical Workflow (PaCW) Ontology



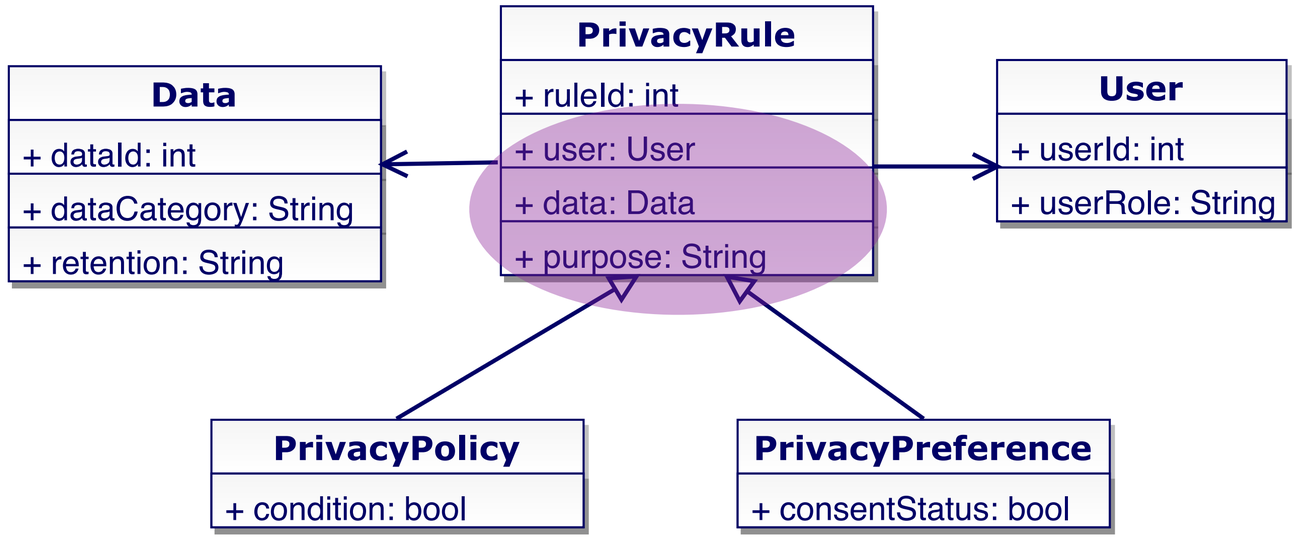
PACW ONTOLOGY

Privacy Domain

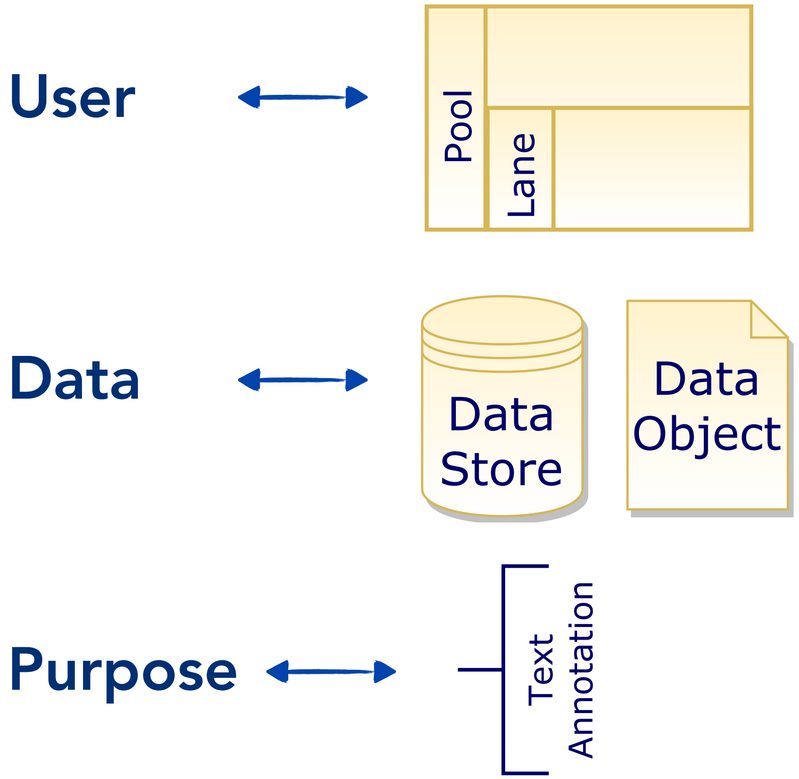


PACW ONTOLOGY

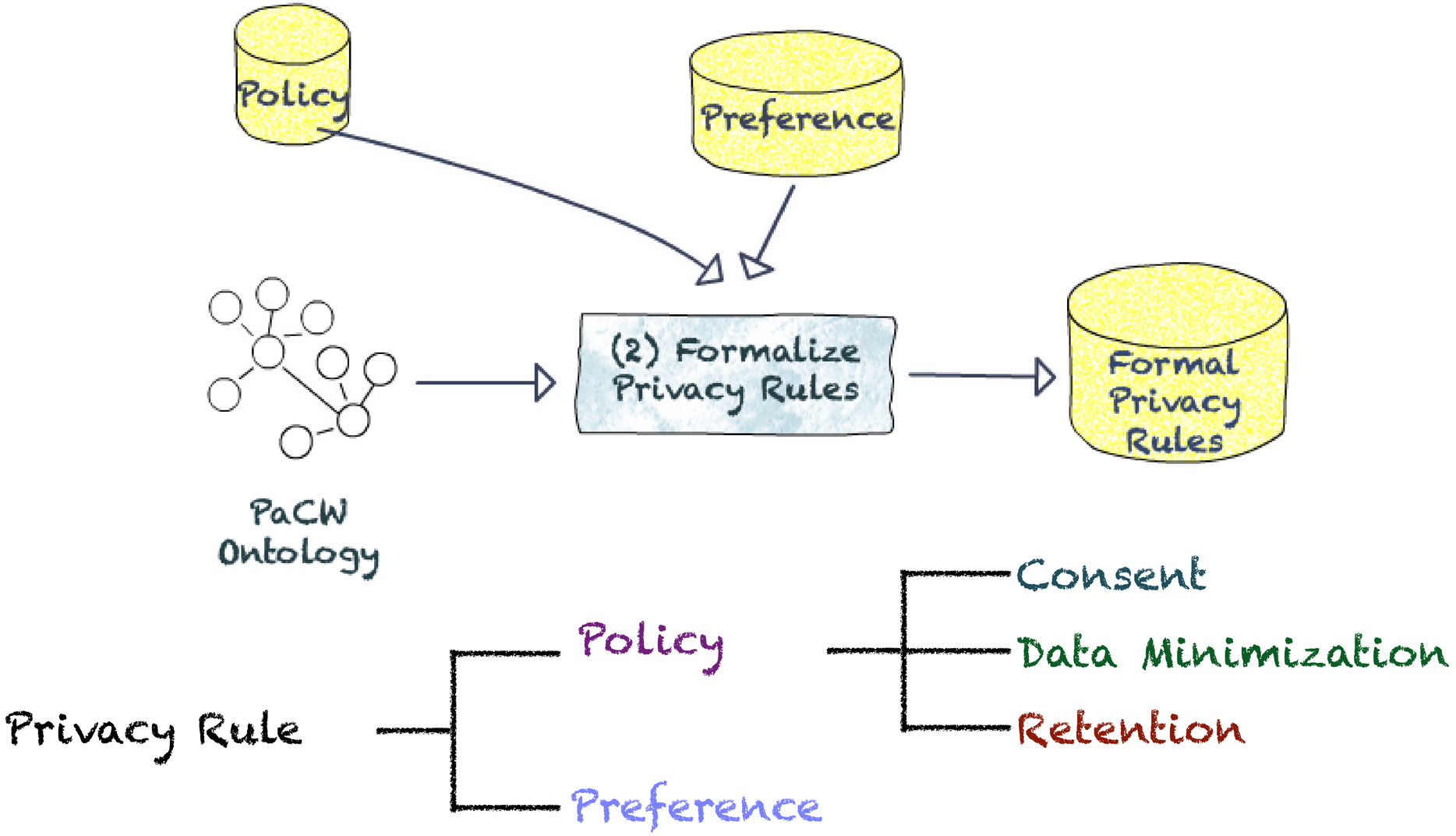
Privacy Domain



Mapping



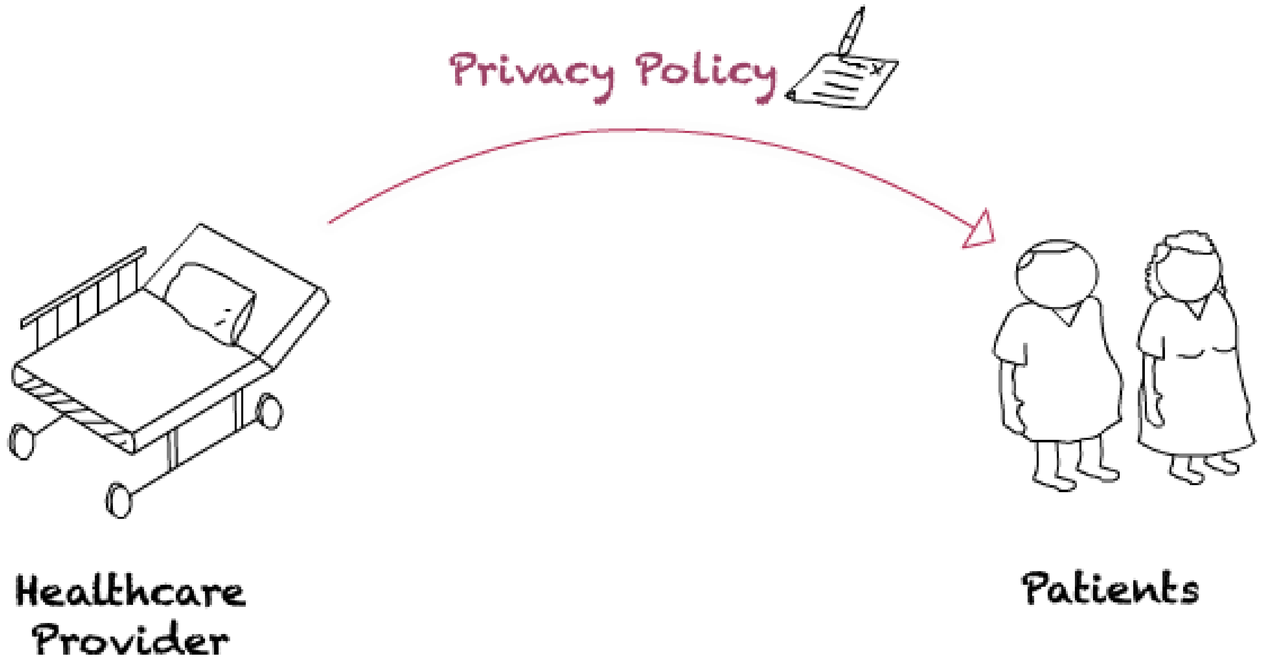
(2) FORMALIZE PRIVACY RULES



PRIVACY POLICY

PRIVACY POLICY

- what data is collected
- who can use it for what purposes
- the modality of data processing, whether it is obligatory or voluntary
- how long it is retained



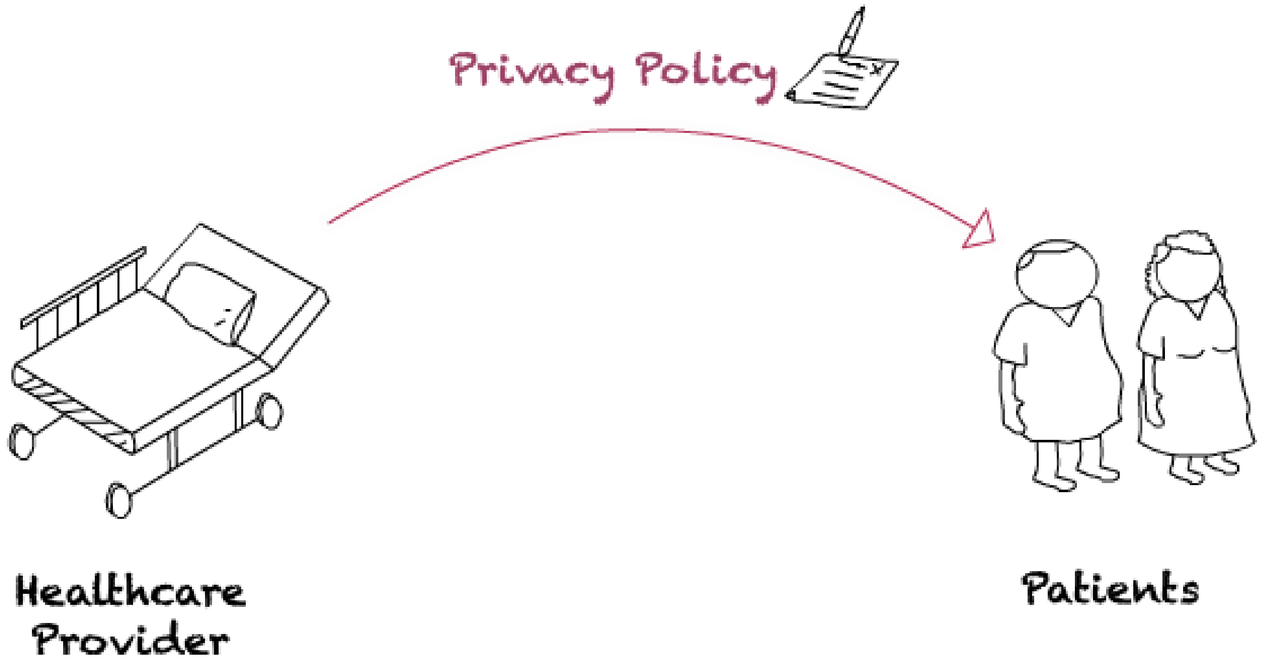
PRIVACY POLICY

- what data is collected
- who can use it for what purposes
- the modality of data processing, whether it is obligatory or voluntary
- how long it is retained

Data Minimization

Consent

Retention



Definition 1 [Consent Privacy Policy]

A consent privacy policy PC consists of rules represented as 2-tuple

pc = (*purpose*, *requiresConsent*), where:

- *purpose* is the reason for which data is accessed;
- *requiresConsent* $\in$ *{true, false}*

Example:

P1: An explicit consent is required for newborn hearing screening.

formal representation ?

Definition 1 [Consent Privacy Policy]

A consent privacy policy PC consists of rules represented as 2-tuple

pc = (*purpose*, *requiresConsent*), where:

- *purpose* is the reason for which data is accessed;
- *requiresConsent* ∈ {*true*, *false*}

Example:

P1: An explicit consent is required for newborn hearing screening.

formal representation ?

Definition 1 [Consent Privacy Policy]

A consent privacy policy PC consists of rules represented as 2-tuple

pc = (*purpose*, *requiresConsent*), where:

- *purpose* is the reason for which data is accessed;
- *requiresConsent* $\in$ *{true, false}*

Example:

P1: An explicit consent is required for newborn hearing screening.

formal representation ?

(newborn-hearing-screening, true)

Definition 2 [Data Minimization Privacy Policy]

A data minimization privacy policy PD consists of rules represented as 4-tuple *pd* = (*user*, *purpose*, *data*, *condition*), where:

- *user* is the set of individuals who access the personal data;
- *data* is a set of data objects;
- *condition* indicates additional conditions.

Example:

P2: A pediatrician can access the result of the lab examination only if the result is abnormal for blood screening.

formal representation ?

Definition 2 [Data Minimization Privacy Policy]

A data minimization privacy policy PD consists of rules represented as 4-tuple *pd = (user, purpose, data, condition)*, where:

- *user* is the set of individuals who access the personal data;
- *data* is a set of data objects;
- *condition* indicates additional conditions.

Example:

P2: A pediatrician can access the result of the lab examination only if the result is abnormal for blood screening.

formal representation ?

Definition 2 [Data Minimization Privacy Policy]

A data minimization privacy policy PD consists of rules represented as 4-tuple *pd = (user, purpose, data, condition)*, where:

- *user* is the set of individuals who access the personal data;
- *data* is a set of data objects;
- *condition* indicates additional conditions.

Example:

P2: A pediatrician can access the result of the lab examination only if the result is abnormal for blood screening.


formal representation ?

(pediatrician, blood-screening, examination-result, examination-result.isAbnormal)

Definition 3 [Retention Privacy Policy]

A retention privacy policy PR consists of rules represented as 4-tuple

r = (*user*, *purpose*, *data*, *retention*), where:

- retention is the period of time the data is stored.

Example:

P3: A hospital can save results for the purpose of hearing screening with a retention limit by 3 years.

formal representation ?

Definition 3 [Retention Privacy Policy]

A retention privacy policy PR consists of rules represented as 4-tuple

r = (*user*, *purpose*, *data*, *retention*), where:

- retention is the period of time the data is stored.

Example:

P3: A hospital can save results for the purpose of hearing screening with a retention limit by 3 years.

formal representation ?

Definition 3 [Retention Privacy Policy]

A retention privacy policy PR consists of rules represented as 4-tuple

r = (*user*, *purpose*, *data*, *retention*), where:

- retention is the period of time the data is stored.

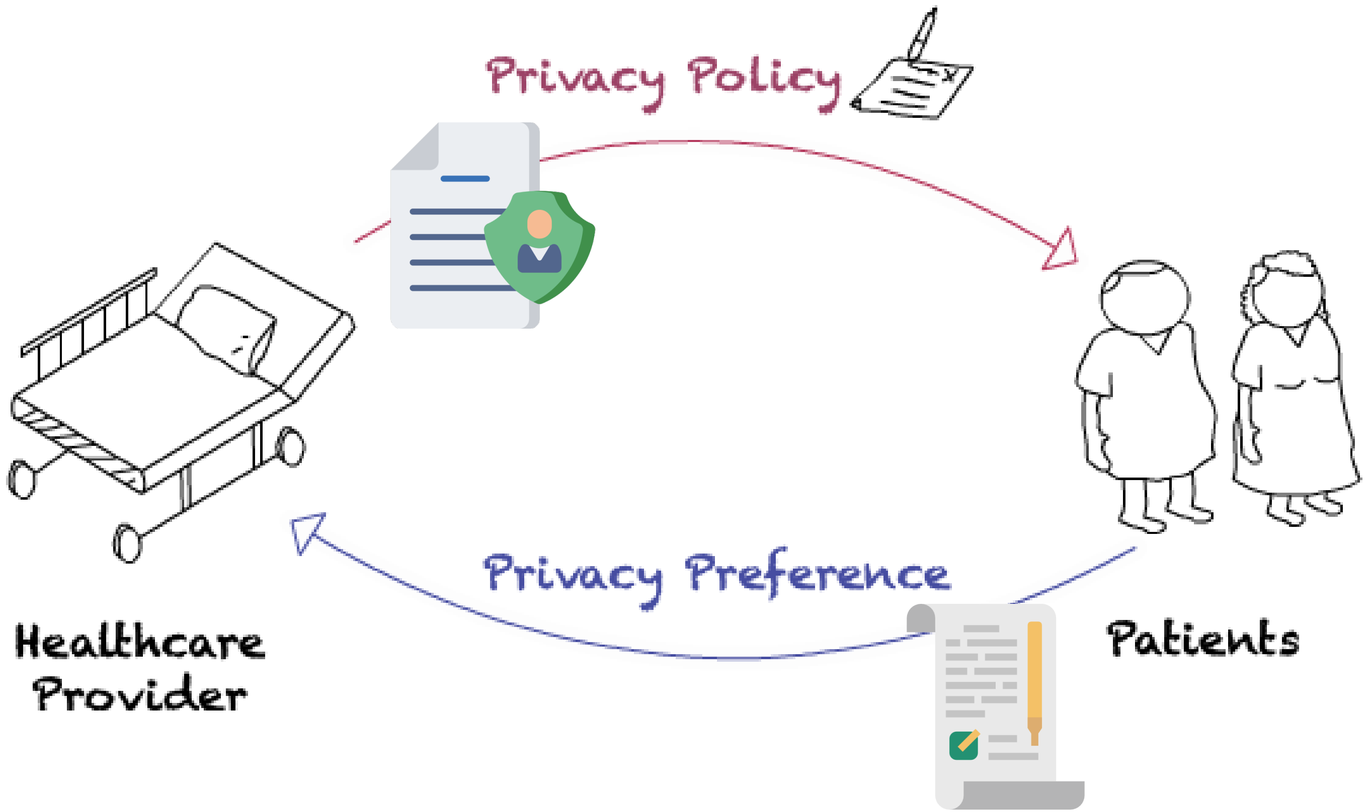
Example:

P3: A hospital can save results for the purpose of hearing screening with a retention limit by 3 years.

formal representation ?

(hospital, hearing-screening, result, 3 years)

Privacy Preference: expresses a data subject's (patients) preferences on sharing / processing their personal data



Definition 4 [Privacy Preference]

A privacy preference R consists of rules represented as 6-tuple

r = (*dataSubject*, *user*, *purpose*, *data*, *duration*, *entryDate*), where:

- *dataSubject* is the individual whom personal data is about;
- *duration* is the duration of preference;
- *entryDate* is the entry date of preference.

Example:

R1: Alice gives consent that only pediatrician Bob can perform hearing screening for 6 months on June 19, 2019.

formal representation ?

Definition 4 [Privacy Preference]

A privacy preference R consists of rules represented as 6-tuple

r = (*dataSubject*, *user*, *purpose*, *data*, *duration*, *entryDate*), where:

- *dataSubject* is the individual whom personal data is about;
- *duration* is the duration of preference;
- *entryDate* is the entry date of preference.

Example:

R1: Alice gives consent that only pediatrician Bob can perform hearing screening for 6 months on June 19, 2019.

formal representation ?

Definition 4 [Privacy Preference]

A privacy preference R consists of rules represented as 6-tuple

r = (*dataSubject*, *user*, *purpose*, *data*, *duration*, *entryDate*), where:

- *dataSubject* is the individual whom personal data is about;
- *duration* is the duration of preference;
- *entryDate* is the entry date of preference.

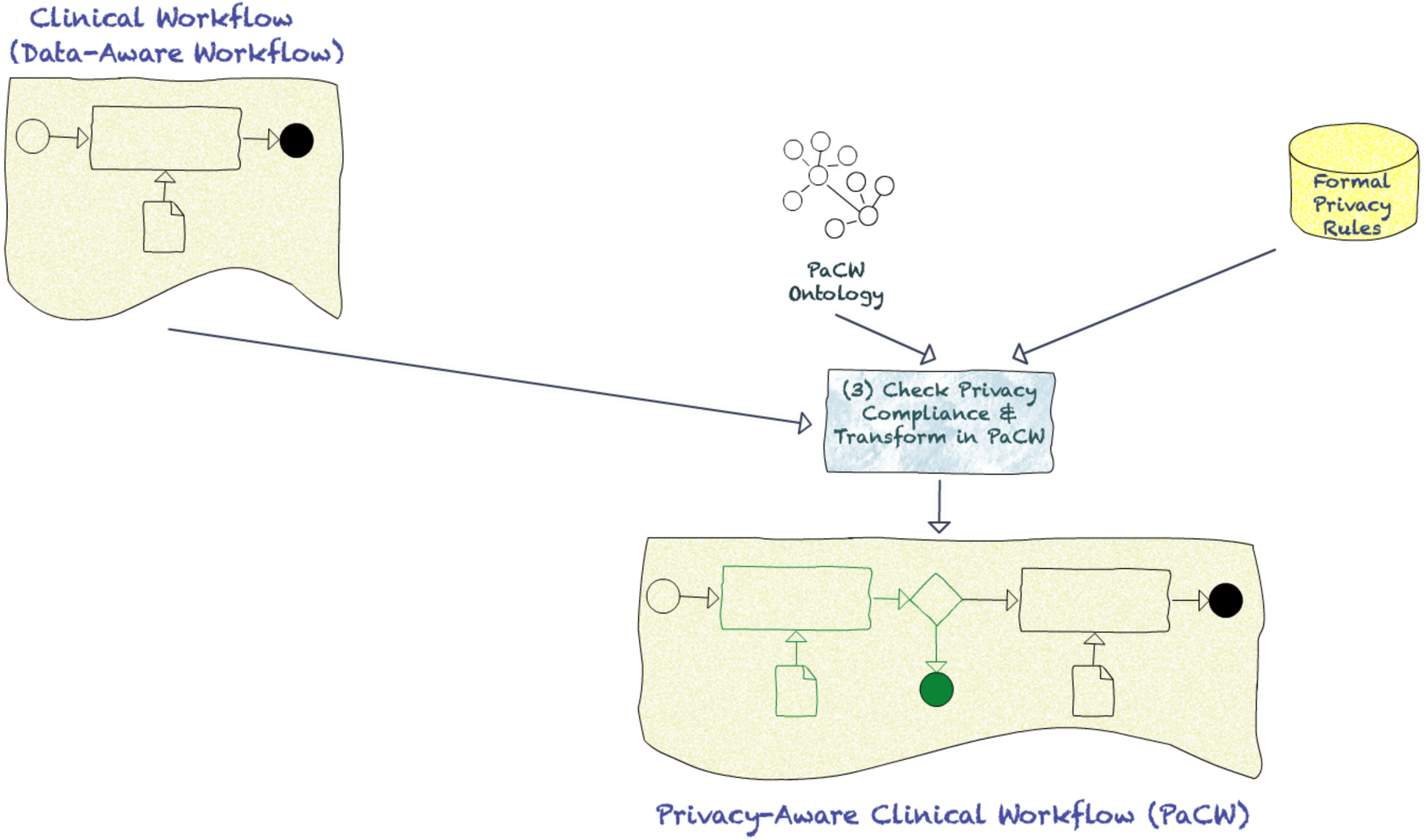
Example:

R1: Alice gives consent that only pediatrician Bob can perform hearing screening for 6 months on June 19, 2019.

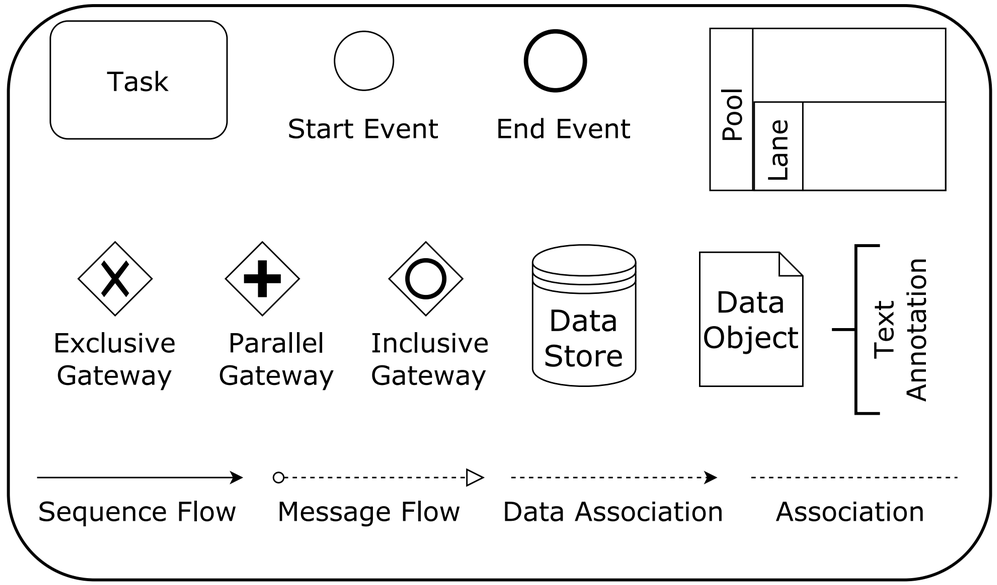
formal representation ?

(Alice, only Bob, hearing-screening, any, 6months, 2019-06-19)

(3) CHECK PRIVACY COMPLIANCE & TRANSFORM INTO PRIVACY-AWARE CLINICAL WORKFLOW (PACW)

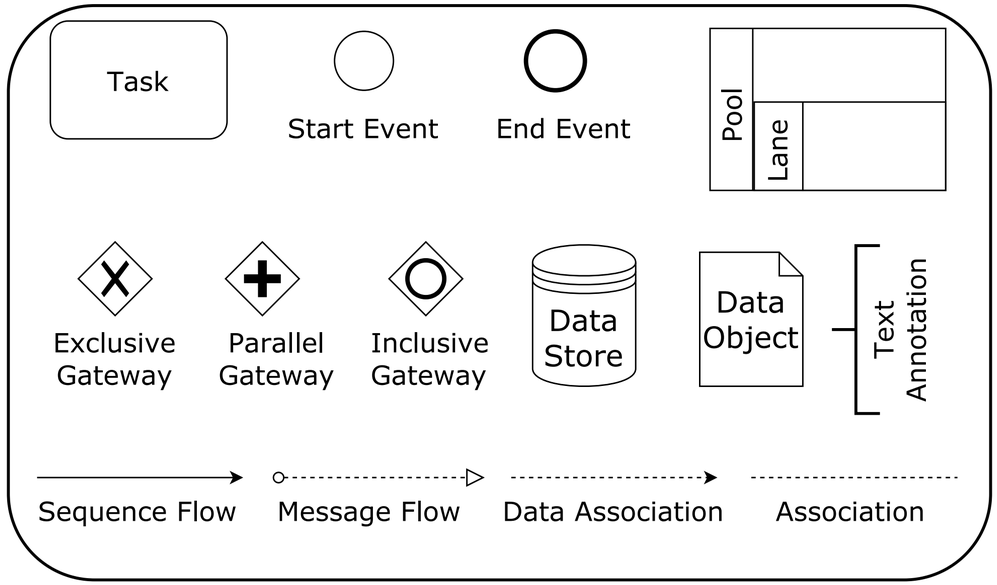


Clinical Workflow

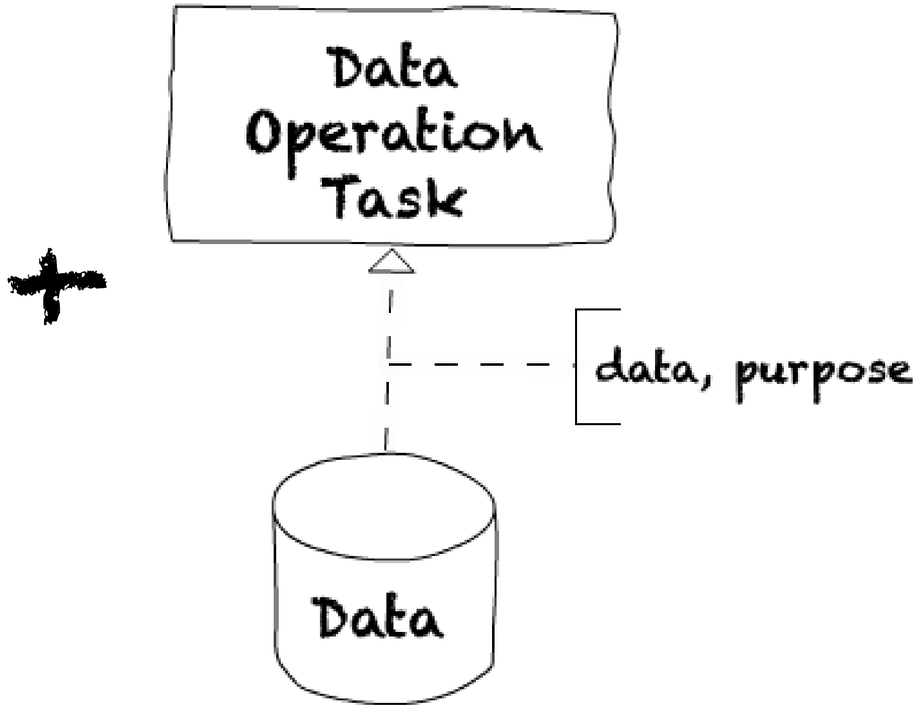


BPMN Core Elements

Clinical Workflow => Data Aware Workflow



BPMN Core Elements



Case

Data-Aware WF + Policy + Data Subject + Preference

Case

Data-Aware WF + Policy + Data Subject + Preference

Privacy-Aware Case

?

Privacy-Aware Case

Data-Aware WF → compliant with Purpose Specification Principle


+

+

+


Data-Aware WF Policy Data Subject Preference → compliant with Consent Check Principle

compliant with Data Minimization Principle

compliant with Limited Retention Principle

Privacy-Aware Case

Data-Aware WF → compliant with Purpose Specification Principle


+

+

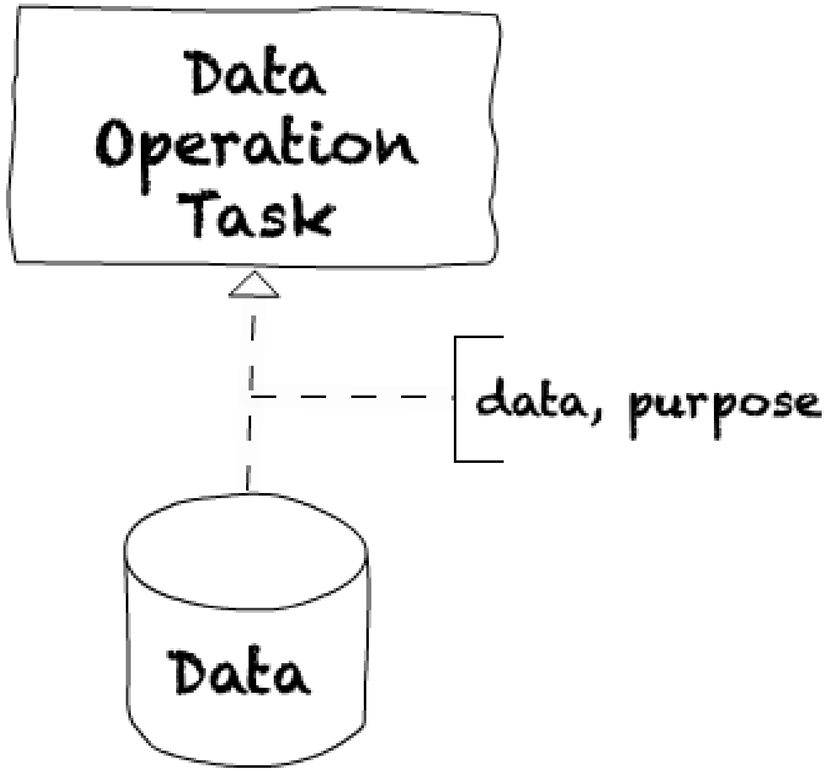
+


Data-Aware WF + Policy + Data Subject + Preference → compliant with Consent Check Principle

compliant with Data Minimization Principle

compliant with Limited Retention Principle

PURPOSE SPECIFICATION COMPLIANCE CHECK



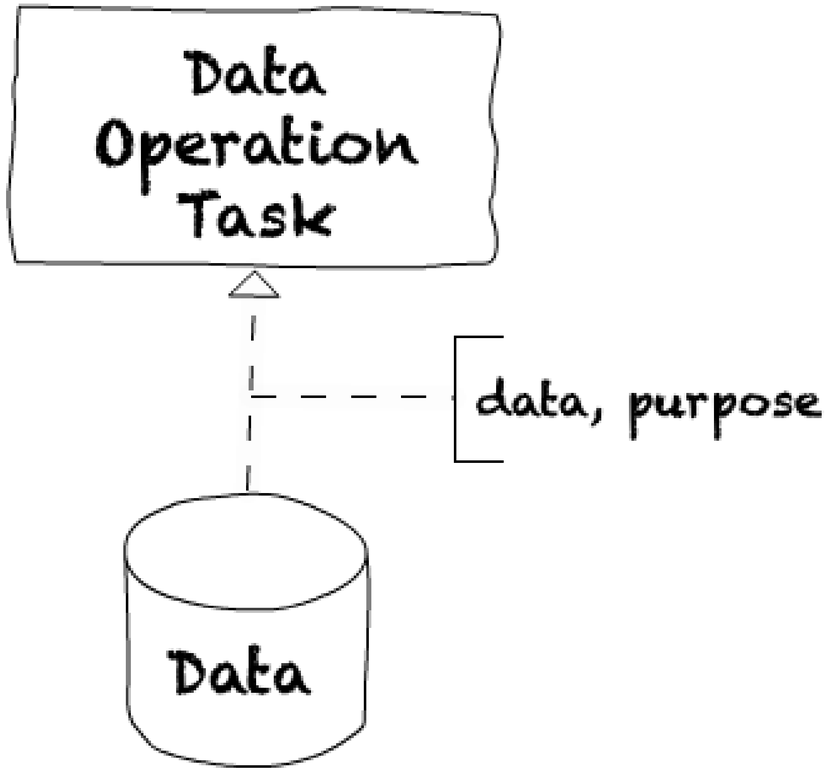
$F \rightarrow$ a set of data associations
$D \rightarrow$ a set of data objects
$p \rightarrow$ a purpose

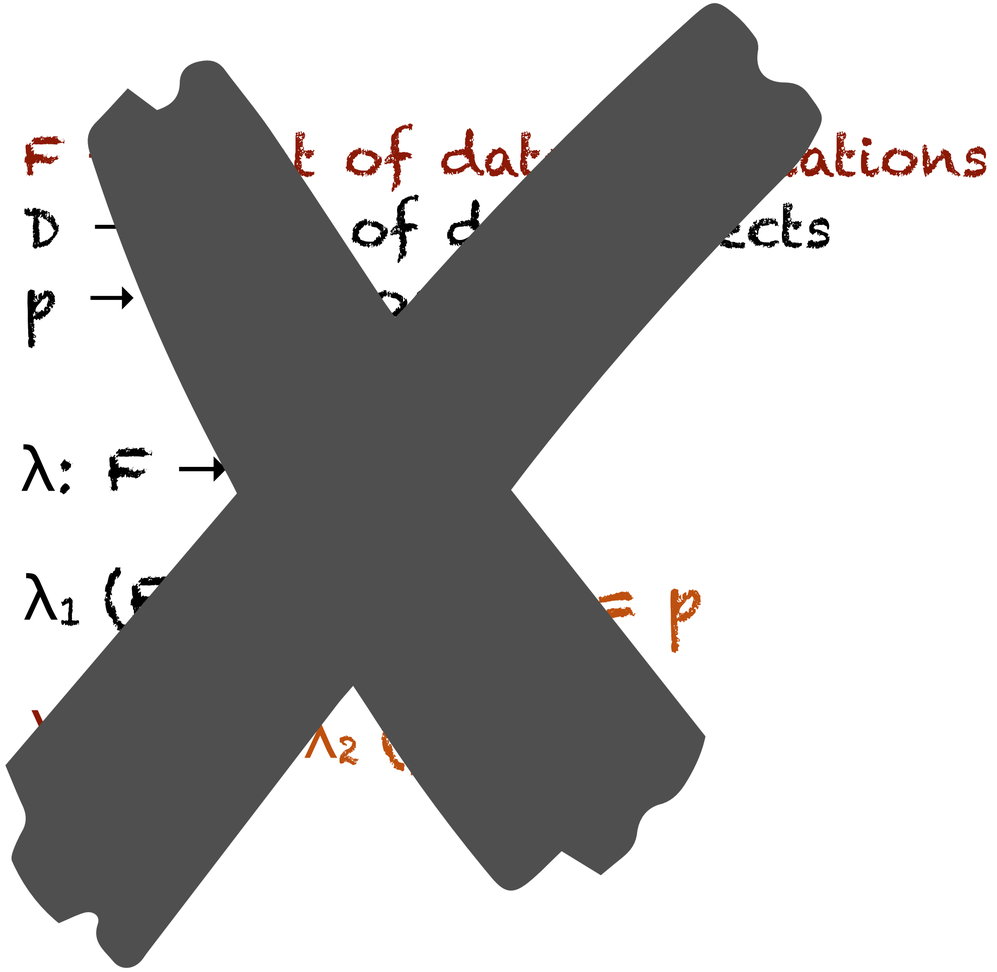
$\lambda: F \rightarrow (D, p)$

$\lambda_1(F) = D, \lambda_2(F) = p$

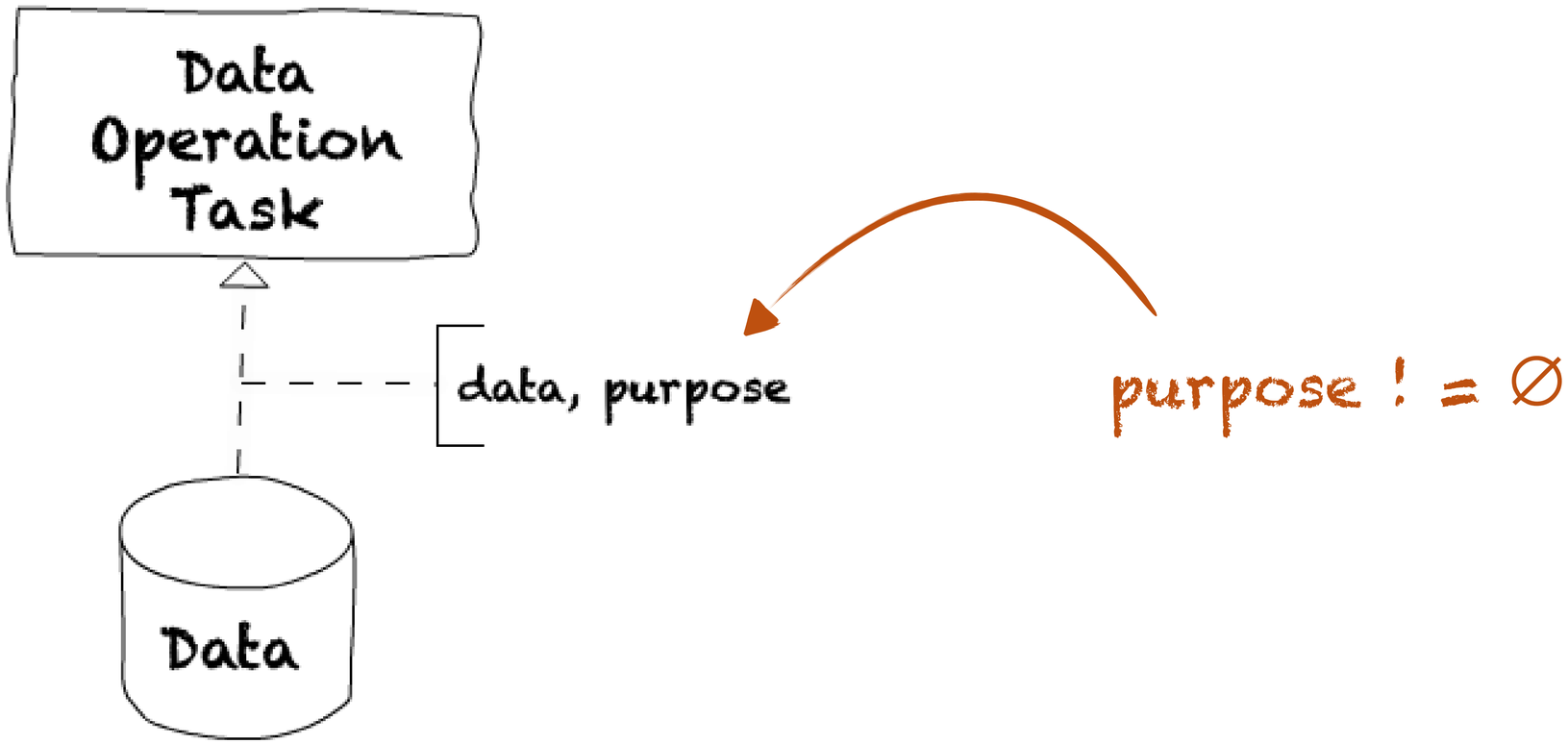
$\forall f \in F, \lambda_2(f) \neq \emptyset$

PURPOSE SPECIFICATION COMPLIANCE CHECK

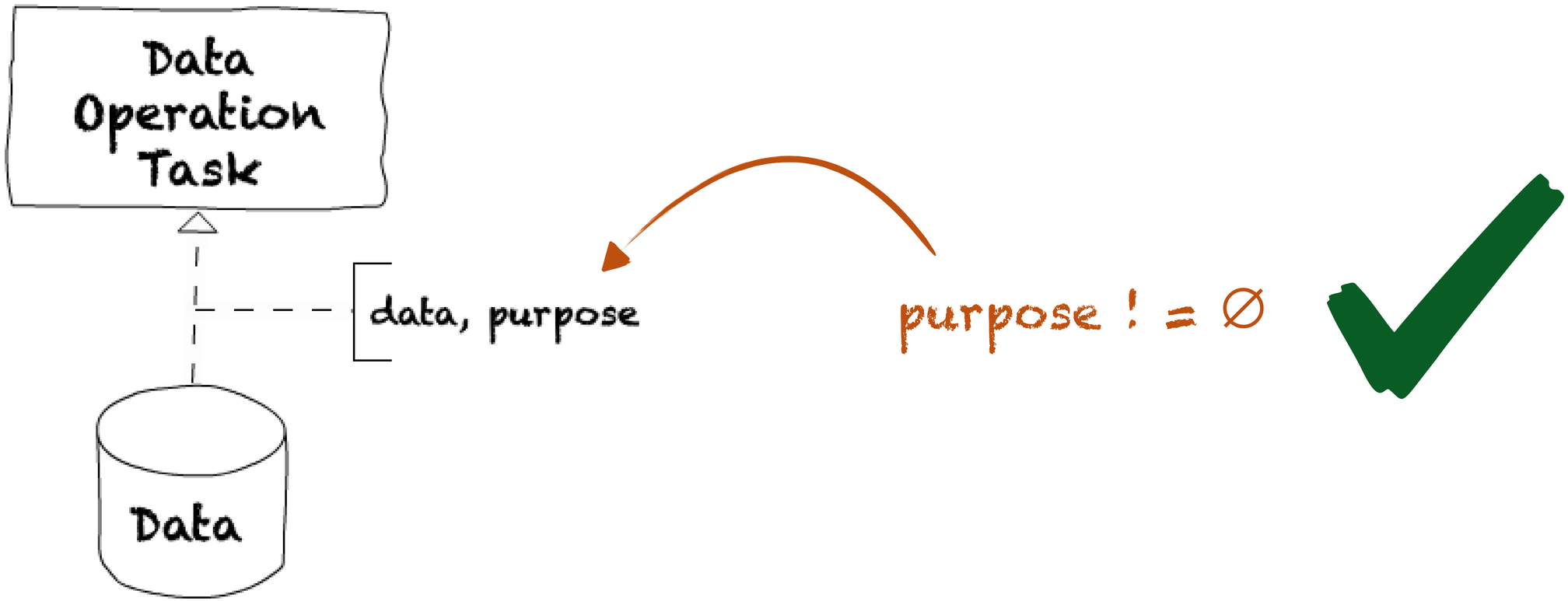




PURPOSE SPECIFICATION COMPLIANCE CHECK

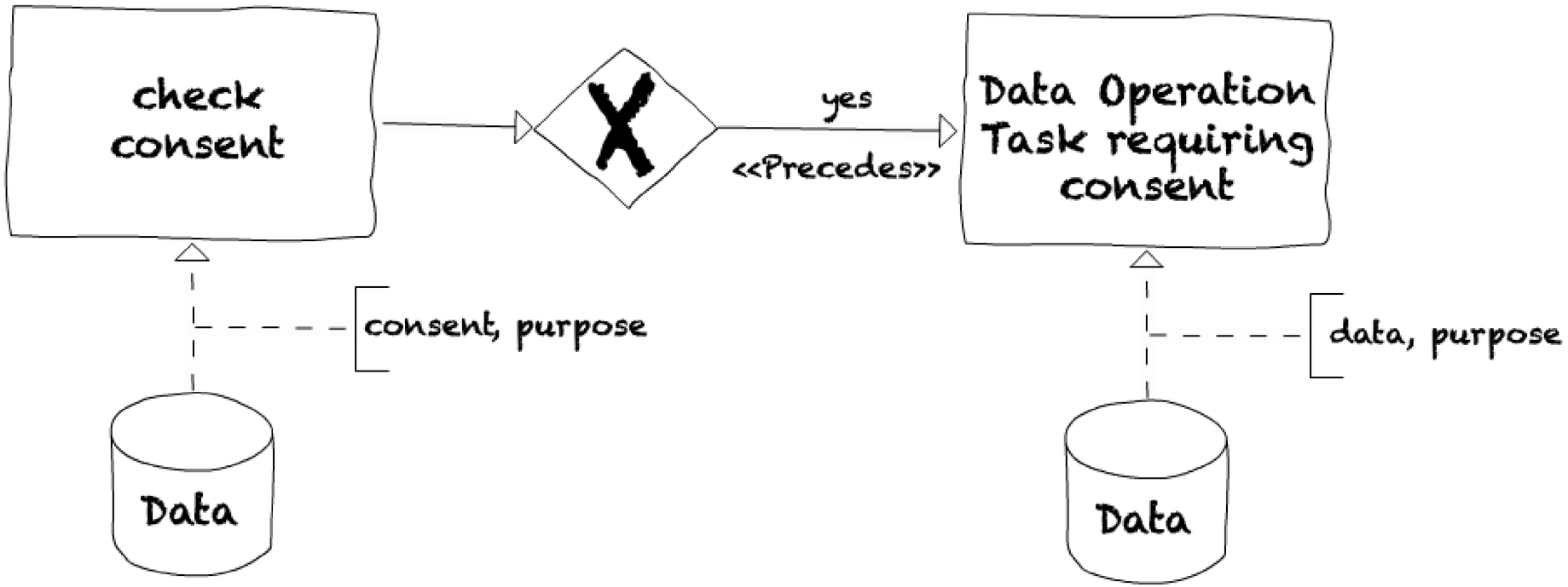


PURPOSE SPECIFICATION COMPLIANCE CHECK



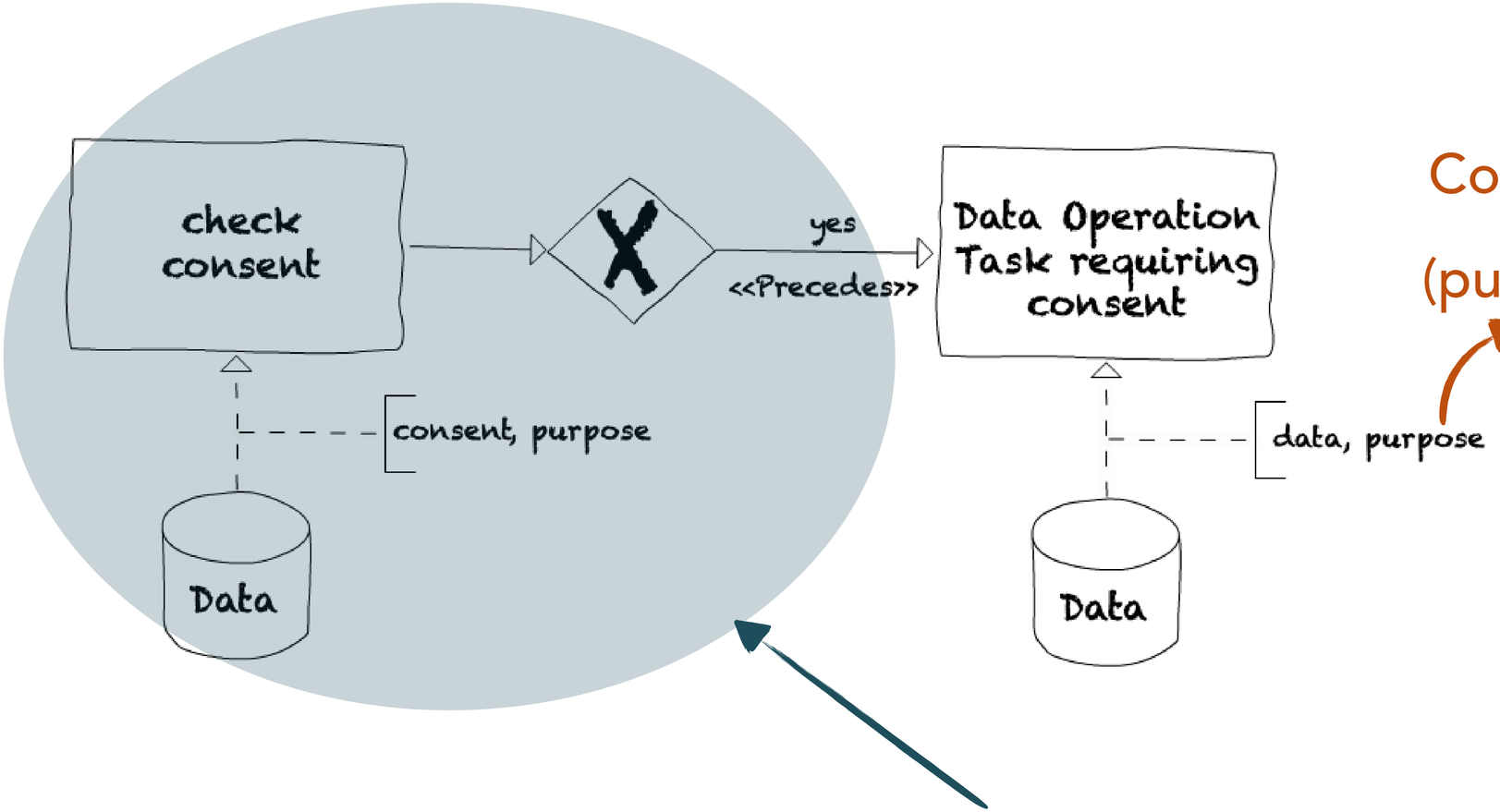
COMPLIANCE WITH CONSENT CHECK (1)

During design time: Consent Check Pattern



A <<Precedes>> B means that B can occur only if A occurred before.

COMPLIANCE WITH CONSENT CHECK (1)

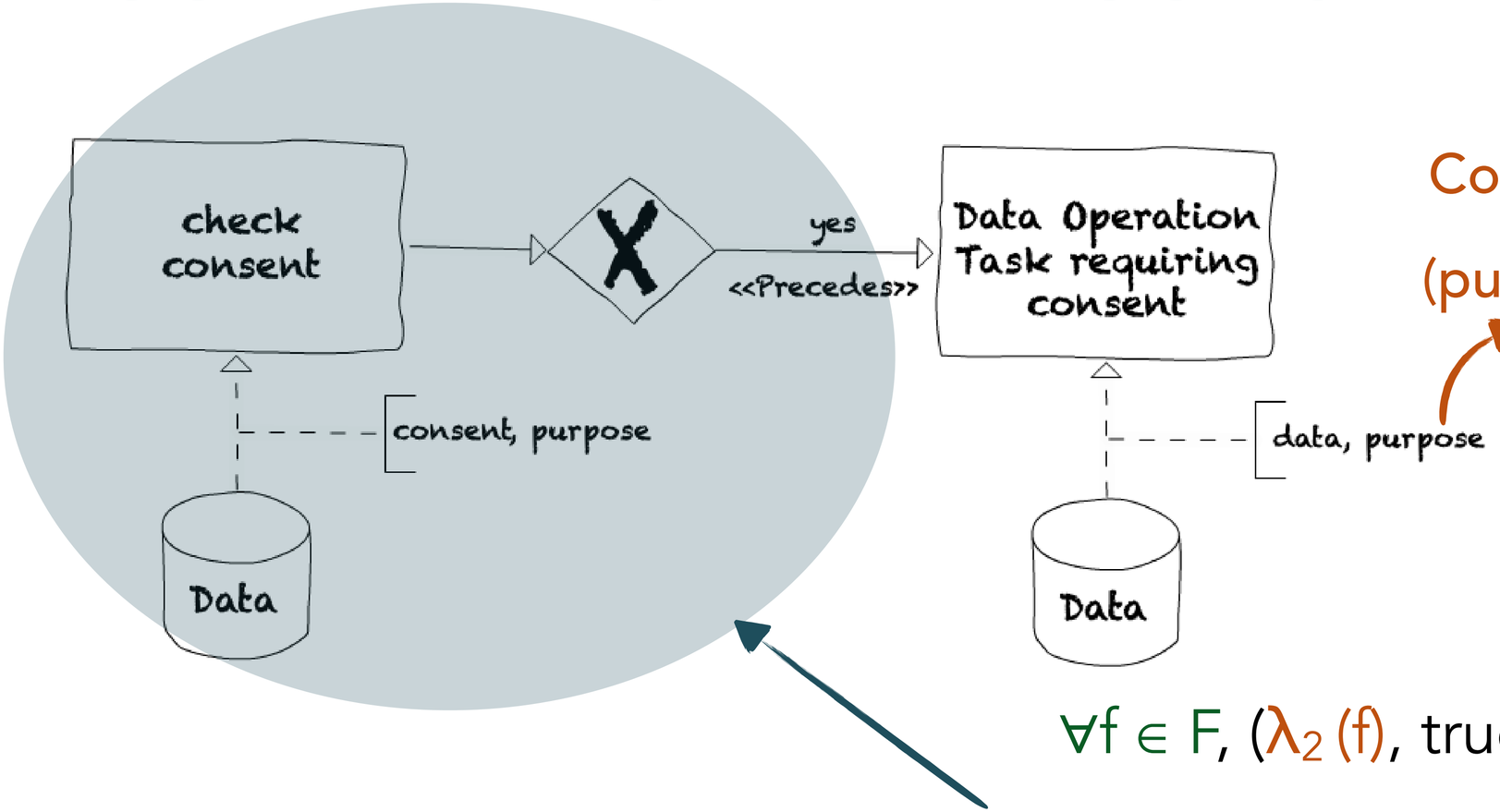


Consent privacy policy includes:

(purpose, requiresConsent = true)

Given a Data-aware WF, check **Consent Check Pattern** predeces Data Operation Task

COMPLIANCE WITH CONSENT CHECK (1)



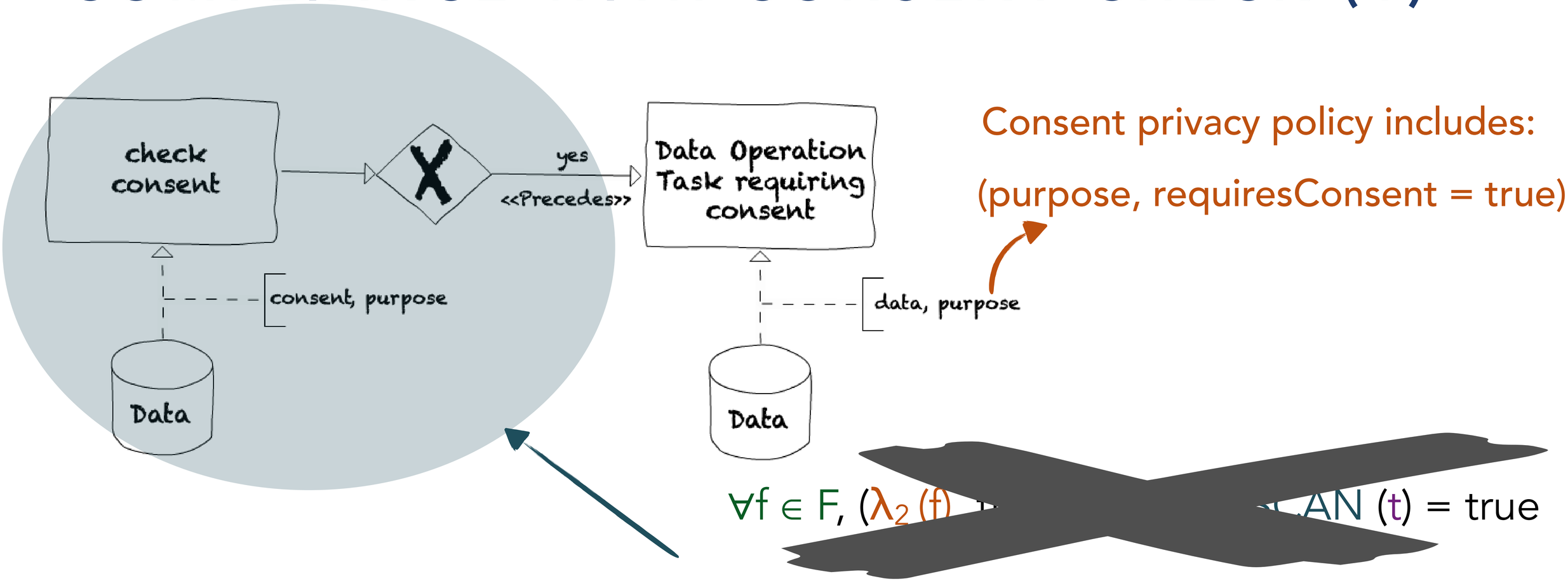
Consent privacy policy includes:

(purpose, requiresConsent = true)

$\forall f \in F, (\lambda_2 (f), true) \in PC \Rightarrow SCAN (t) = true$

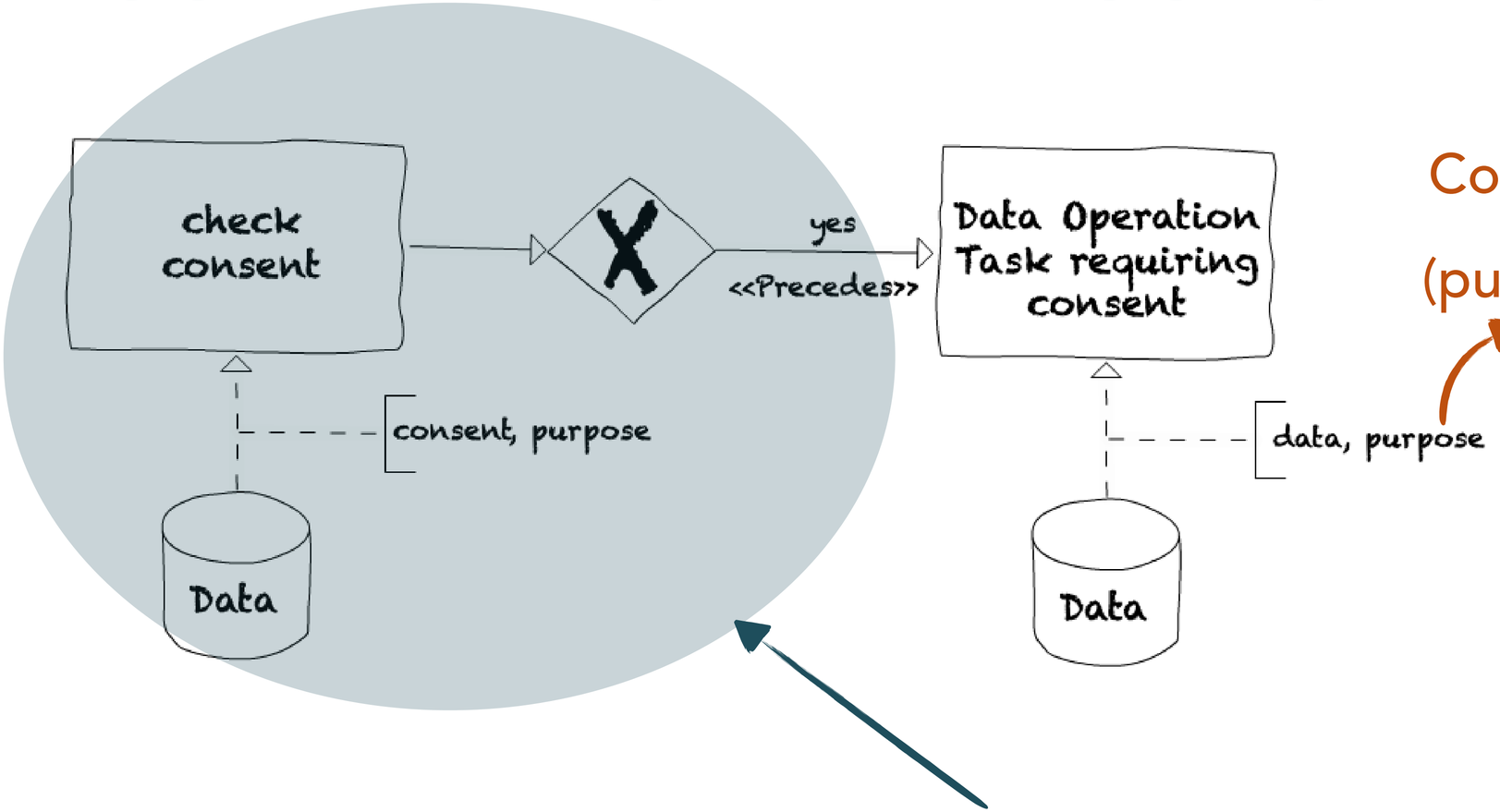
Given a Data-aware WF, check **Consent Check Pattern** predeces Data Operation Task

COMPLIANCE WITH CONSENT CHECK (1)



Given a Data-aware WF, check **Consent Check Pattern** predeces Data Operation Task

COMPLIANCE WITH CONSENT CHECK (1)



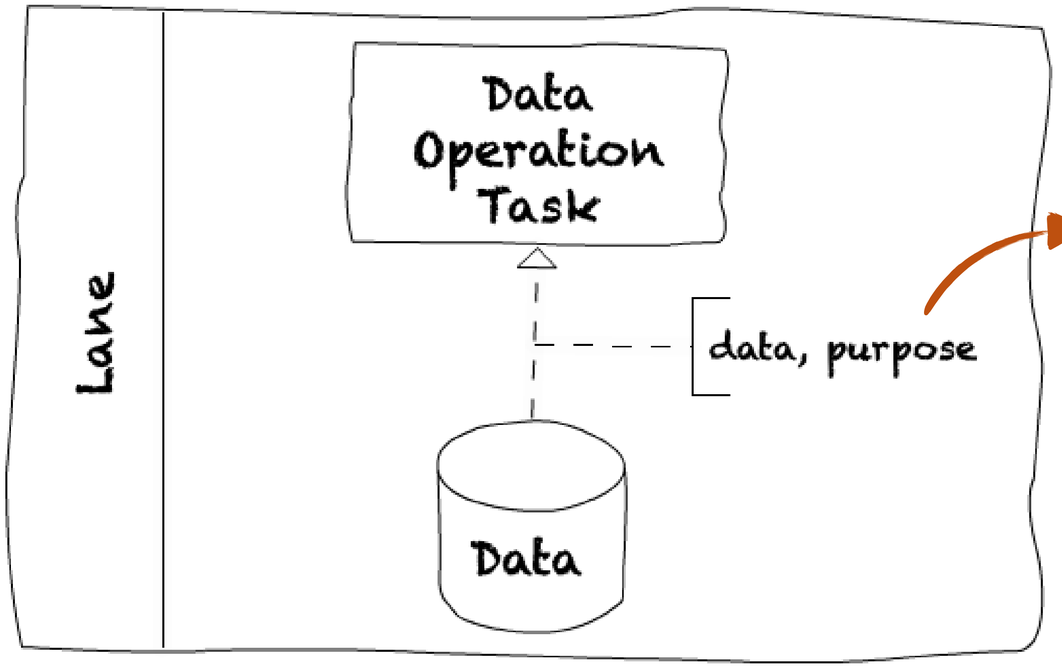
Consent privacy policy includes:

(purpose, requiresConsent = true)

Given a Data-aware WF, check **Consent Check Pattern** predeces Data Operation Task

created a function traversing all sequence flows reaching Data Operation Task

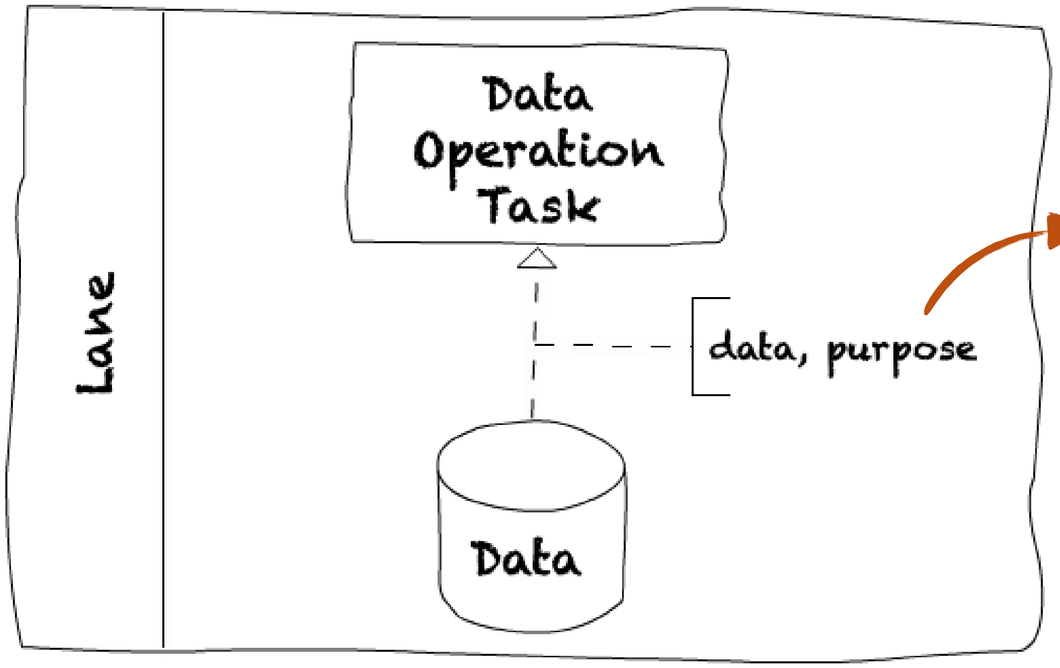
COMPLIANCE WITH CONSENT CHECK (2)



Consent privacy policy includes:

(purpose, requiresConsent = true)

COMPLIANCE WITH CONSENT CHECK (2)



Consent privacy policy includes:

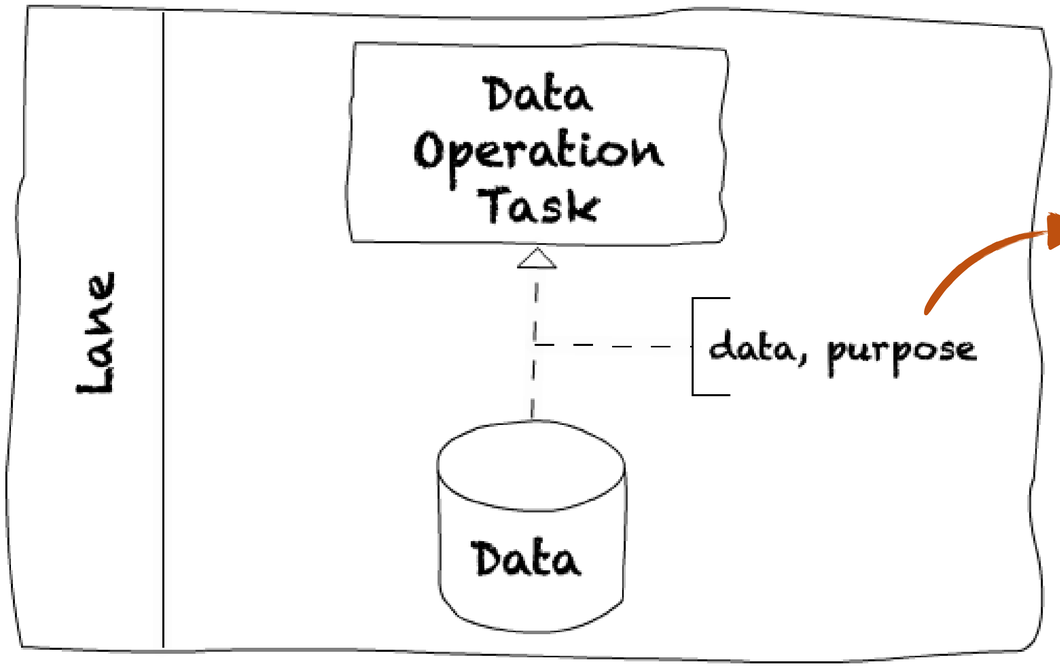
(purpose, requiresConsent = true)

During run time: Check Privacy Preferences

+

DataSubject **Preference**

COMPLIANCE WITH CONSENT CHECK (2)



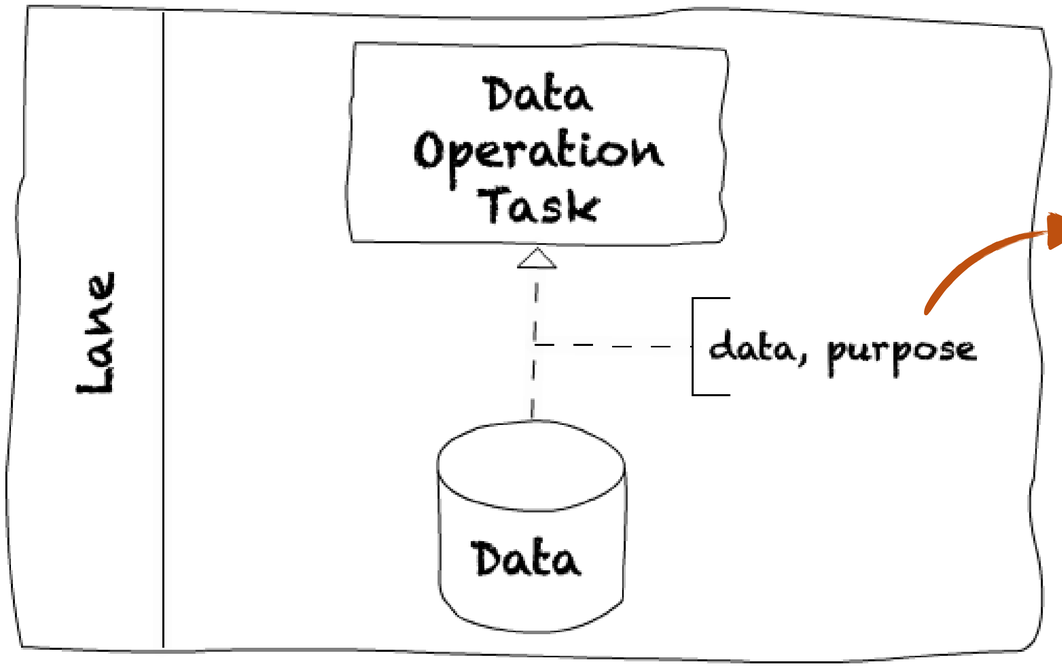
Consent privacy policy includes:

(purpose, requiresConsent = true)

During run time: Check Privacy Preferences

DataSubject **Preference**

COMPLIANCE WITH CONSENT CHECK (2)



Consent privacy policy includes:

(purpose, requiresConsent = true)

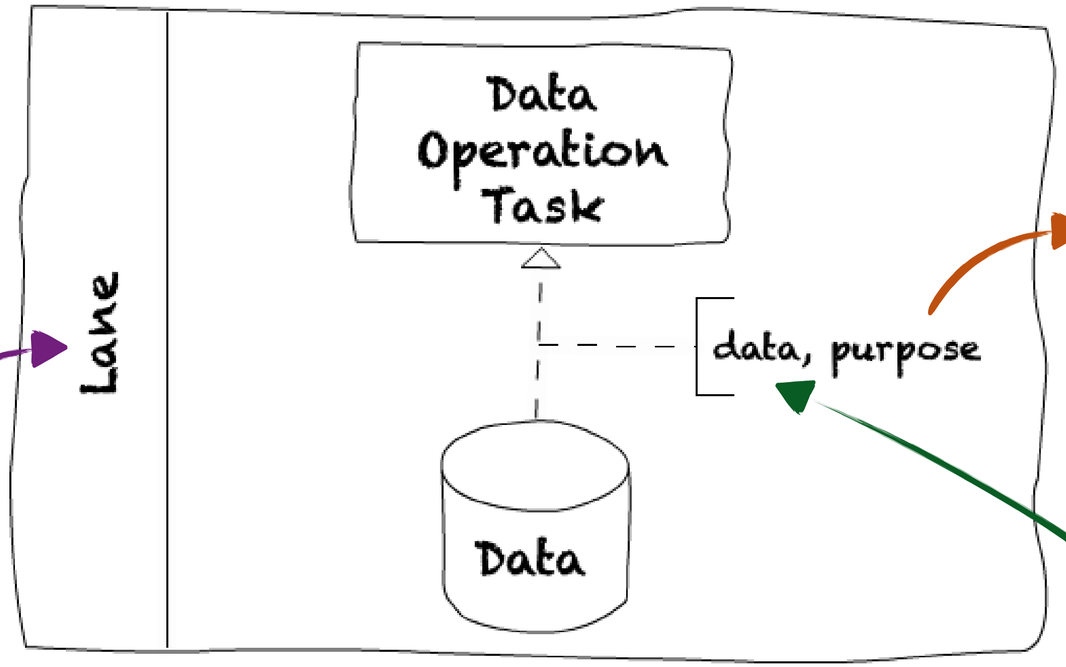
During run time: Check Privacy Preferences

DataSubject

Preference

r = (*DataSubject*, *user*, *purpose*, *data*, *duration*, *entryDate*) ?

COMPLIANCE WITH CONSENT CHECK (2)



Consent privacy policy includes:

(purpose, requiresConsent = true)

During run time: Check Privacy Preferences

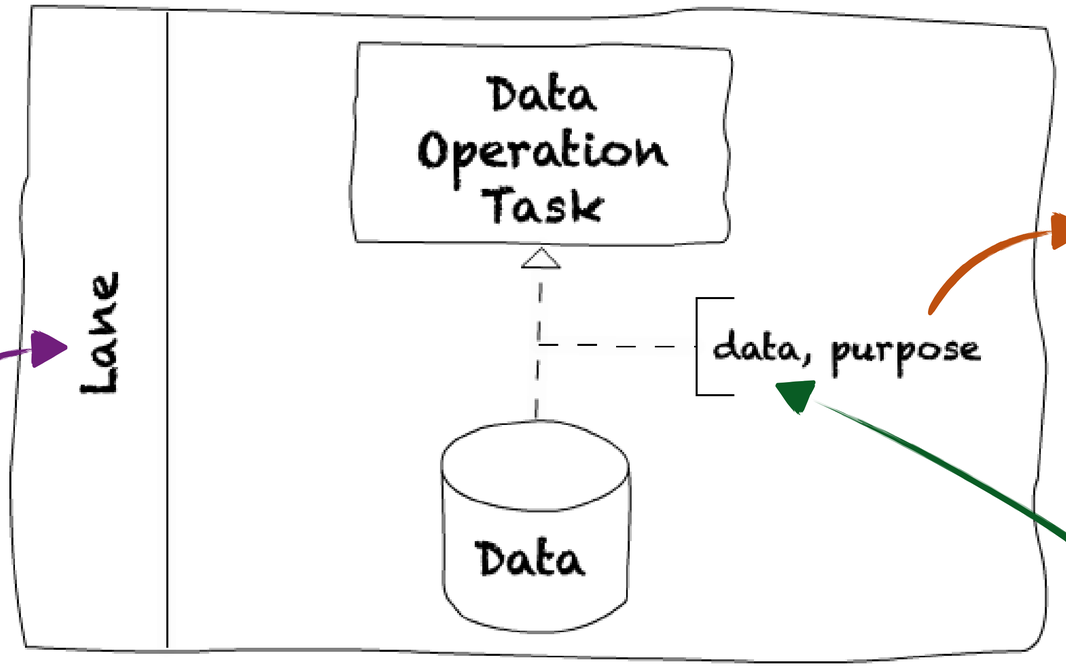
DataSubject

+

Preference

r = (*DataSubject*, *user*, *purpose*, *data*, *duration*, *entryDate*) ?

COMPLIANCE WITH CONSENT CHECK (2)



user

Consent privacy policy includes:

(purpose, requiresConsent = true)

During run time: Check Privacy Preferences

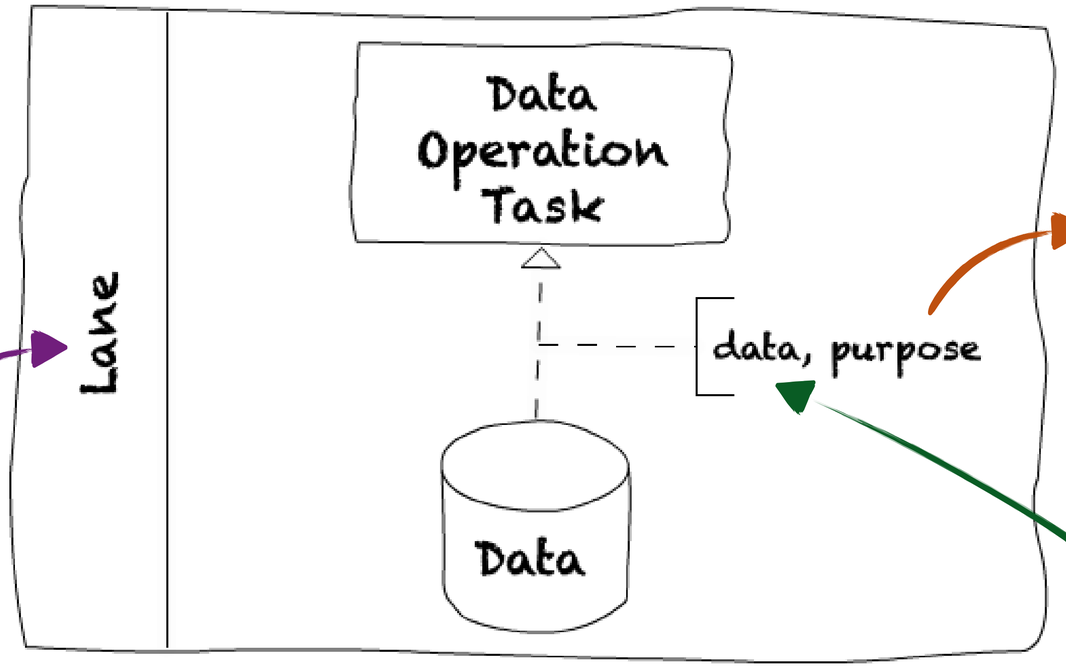
DataSubject

+

Preference

r = (*DataSubject*, *user*, *purpose*, *data*, *duration*, *entryDate*) ?

COMPLIANCE WITH CONSENT CHECK (2)



user

Consent privacy policy includes:

(purpose, requiresConsent = true)

today - entryDate >= duration

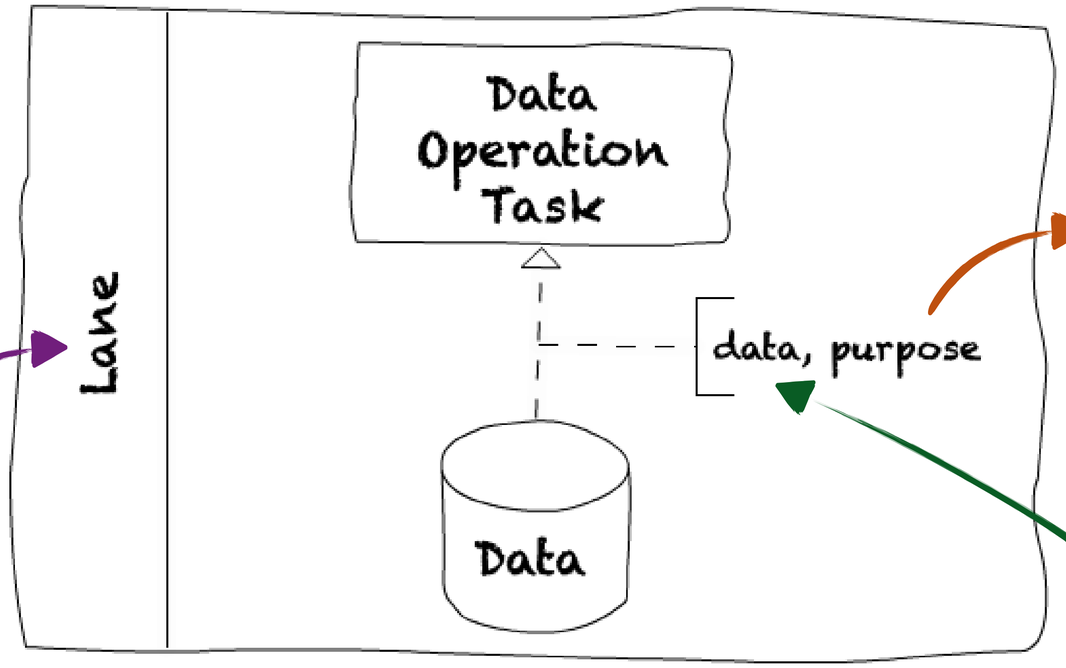
During run time: Check Privacy Preferences

+

r = (DataSubject, user, purpose, data, duration, entryDate) ?

DataSubject **Preference**

COMPLIANCE WITH CONSENT CHECK (2)



user

Consent privacy policy includes:

(purpose, requiresConsent = true)

today - entryDate >= duration

valid ✓

During run time: Check Privacy Preferences

DataSubject

+

Preference

r = (DataSubject, user, purpose, data, duration, entryDate) ✓

TRANSFORMATION

predefined transformation actions for the privacy violations

captured during compliance check

Purpose Specification: *at least one specific purpose* for each data operation

TRANSFORMATION

predefined transformation actions for the privacy violations

captured during compliance check

Purpose Specification: *at least one specific purpose* for each data operation

When no purpose specified → *privacy violation*

transformation action → return message as a warning

TRANSFORMATION - CONSENT CHECK

Some tasks are legitimate only with an **explicit consent** of a data subject.

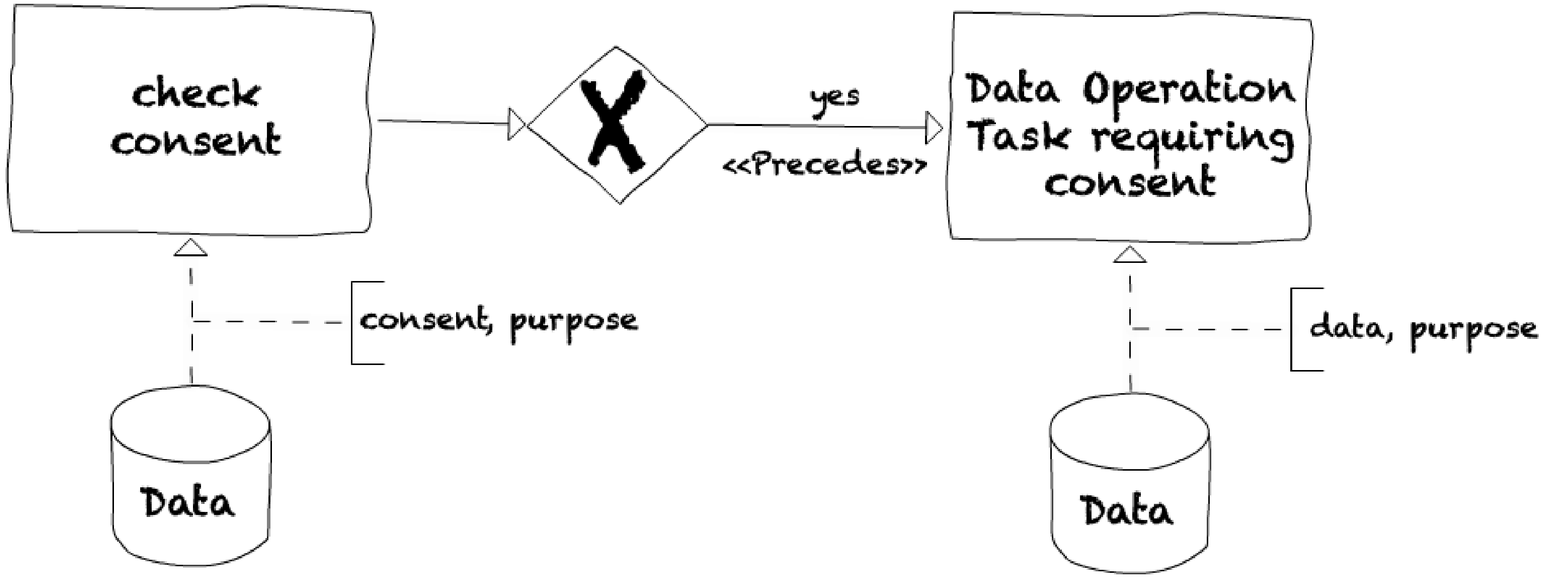
consent required, but no consent → *privacy violation*

TRANSFORMATION - CONSENT CHECK

Some tasks are legitimate only with an **explicit consent** of a data subject.

consent required, but no consent → *privacy violation*

transformation action → adding consent check pattern beforehand

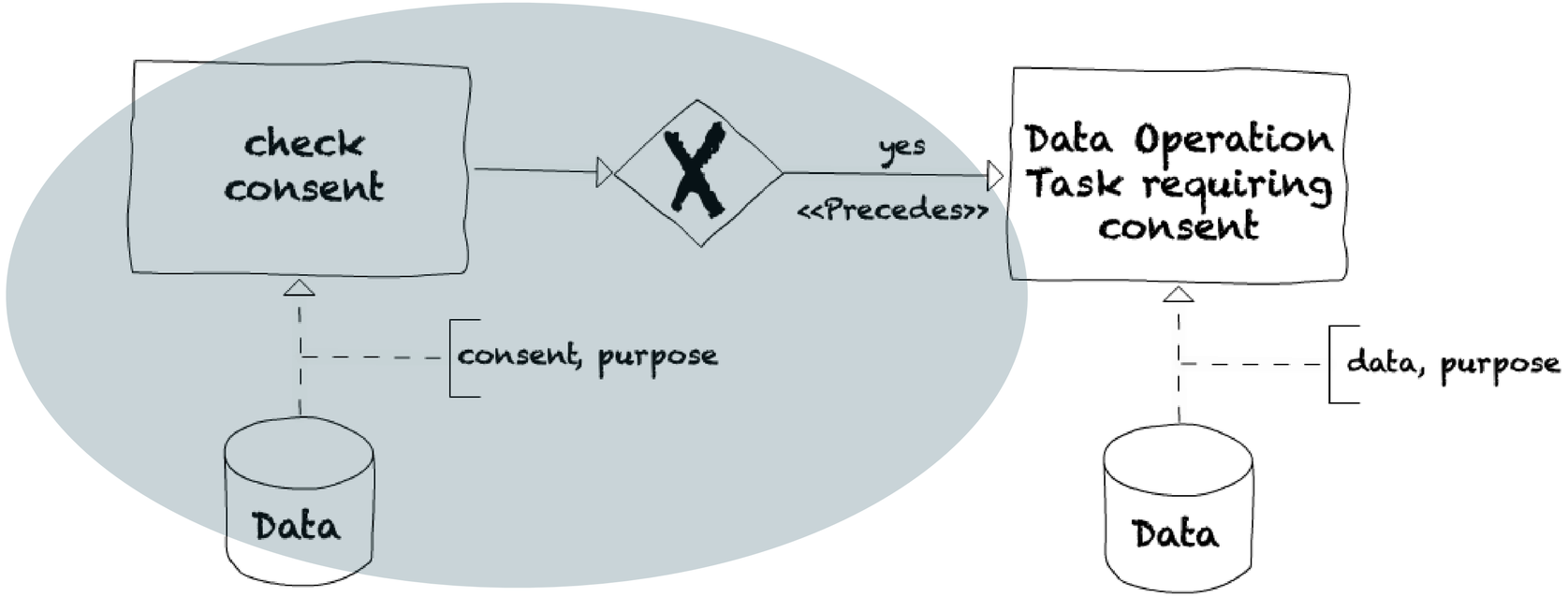


TRANSFORMATION - CONSENT CHECK

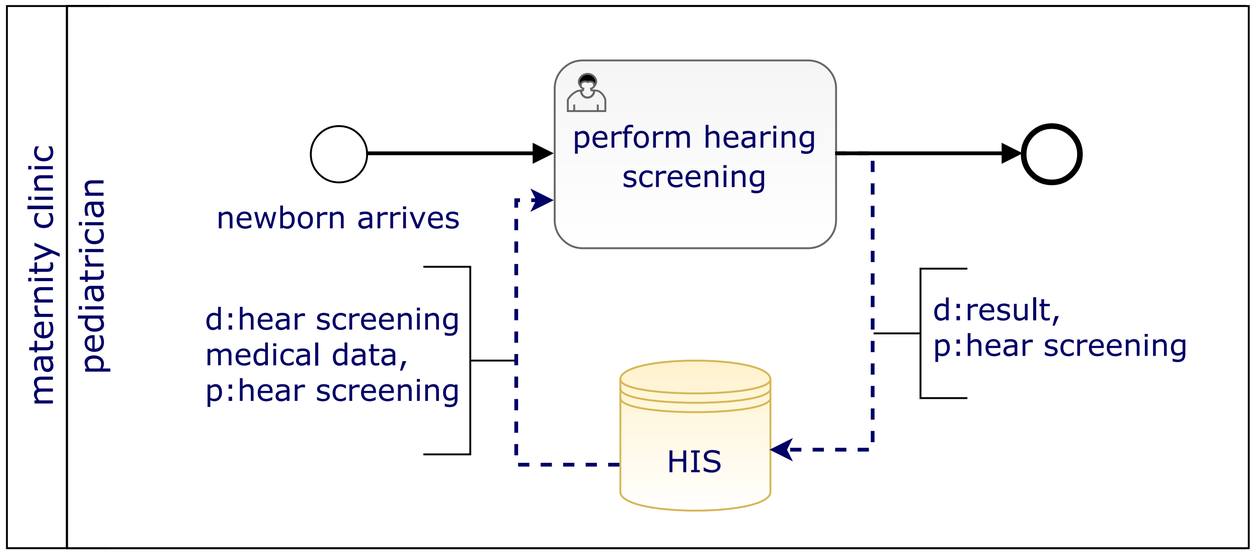
Some tasks are legitimate only with an **explicit consent** of a data subject.

consent required, but no consent → *privacy violation*

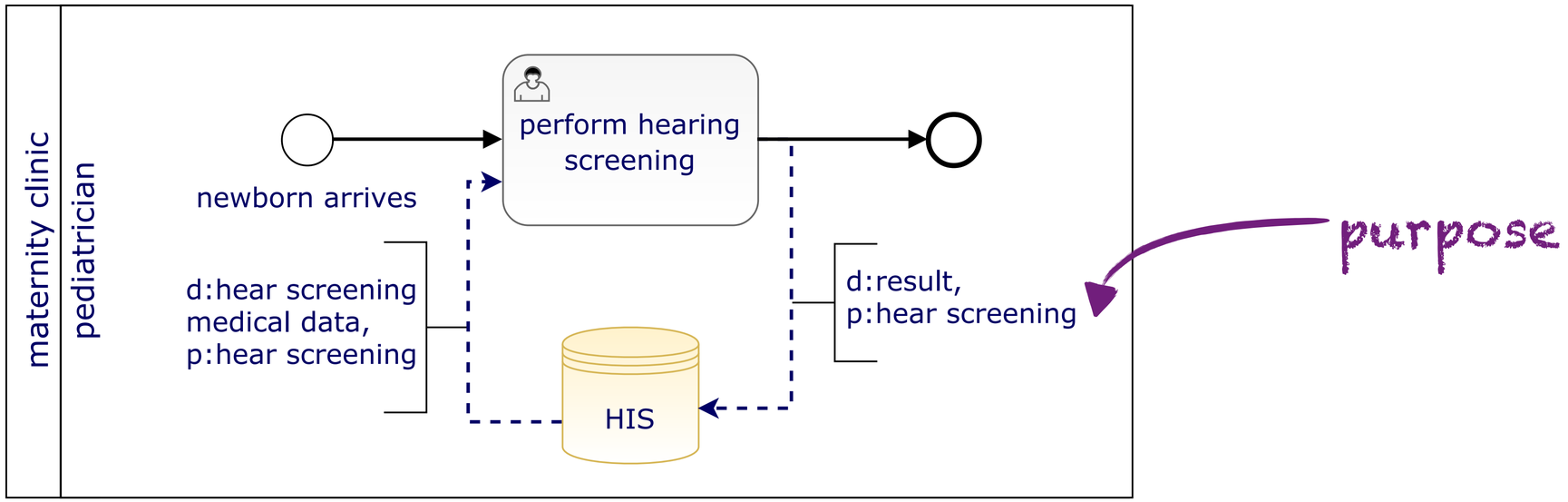
transformation action → adding consent check pattern beforehand



EXAMPLE: HEARING PROCEDURE - *BEFORE TRANSFORMATION*



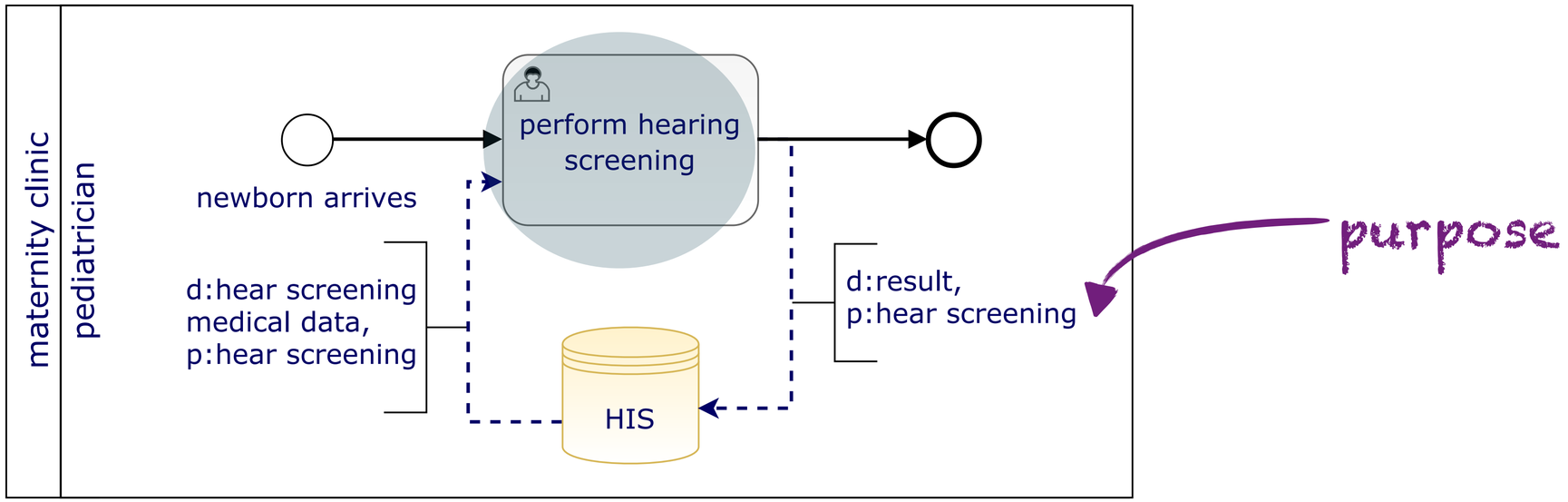
EXAMPLE: HEARING PROCEDURE - *BEFORE TRANSFORMATION*



P1: An explicit consent is required for newborn hearing screening procedure.

(hearing-screening, true) ∈ Consent Policy

EXAMPLE: HEARING PROCEDURE - *BEFORE TRANSFORMATION*

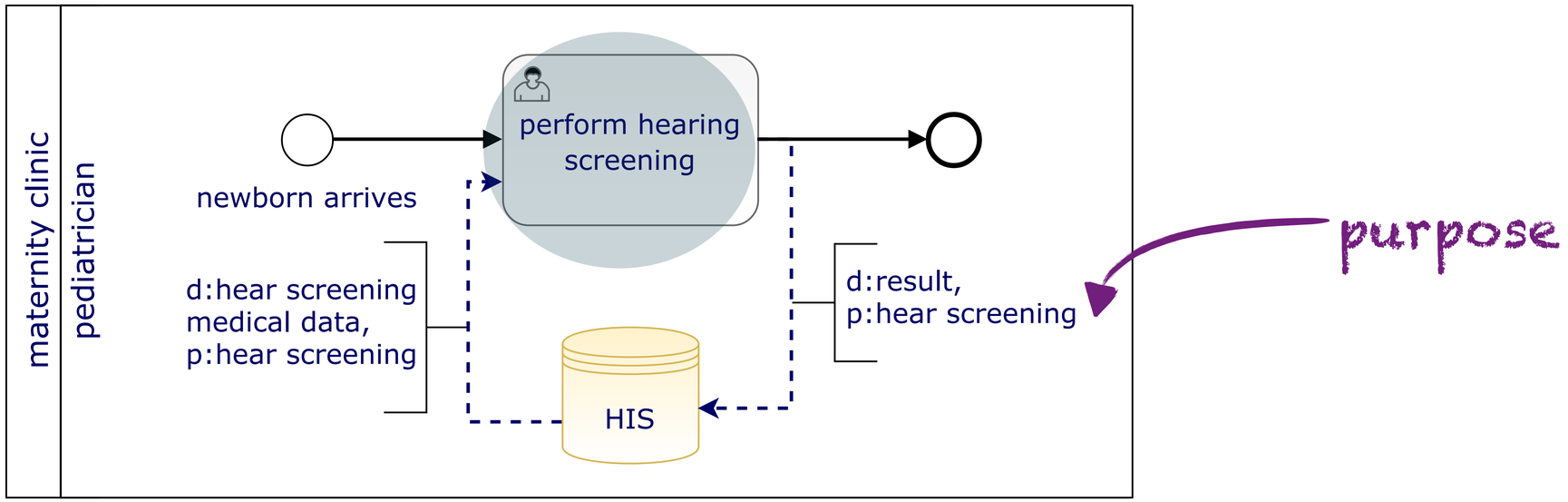


P1: An explicit consent is required for newborn hearing screening procedure.

(hearing-screening, true) ∈ Consent Policy

check **Consent Check Pattern** predeces "perform hearing screening" ?

EXAMPLE: HEARING PROCEDURE - *BEFORE TRANSFORMATION*



P1: An explicit consent is required for newborn hearing screening procedure.

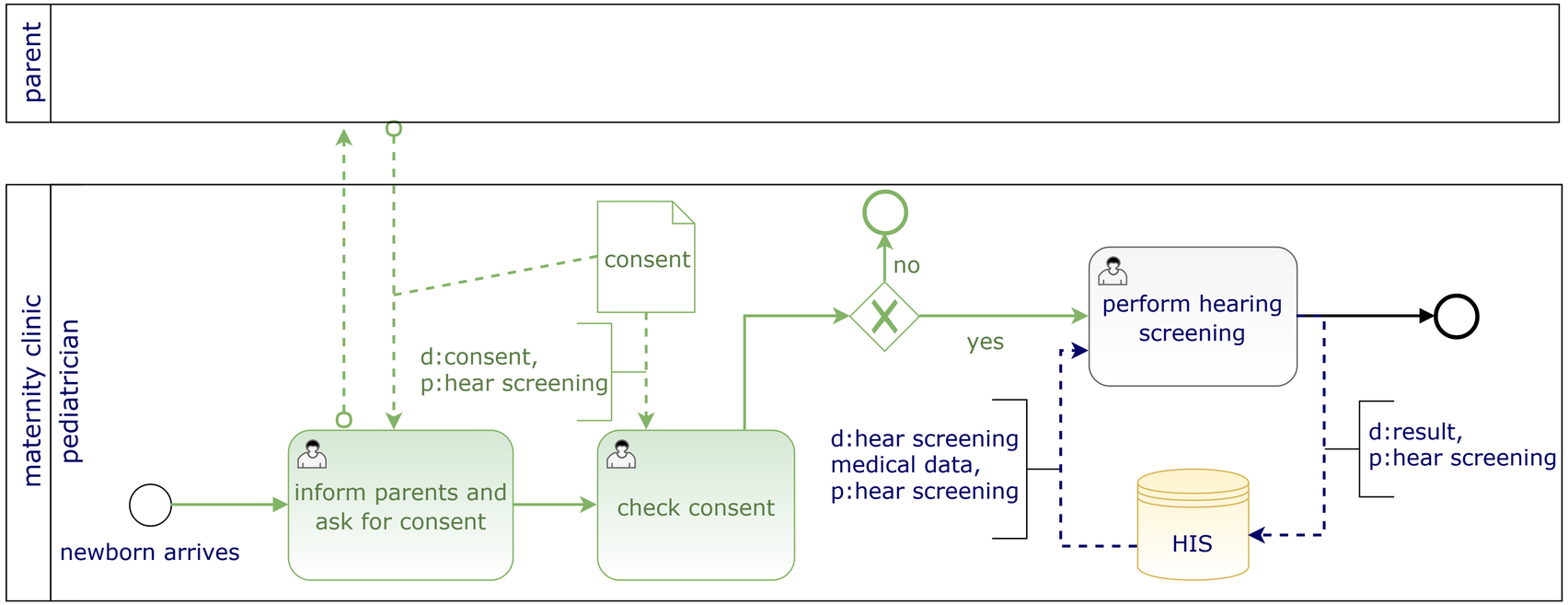
(hearing-screening, true) ∈ Consent Policy

check **Consent Check Pattern** predeces "perform hearing screening" ✗

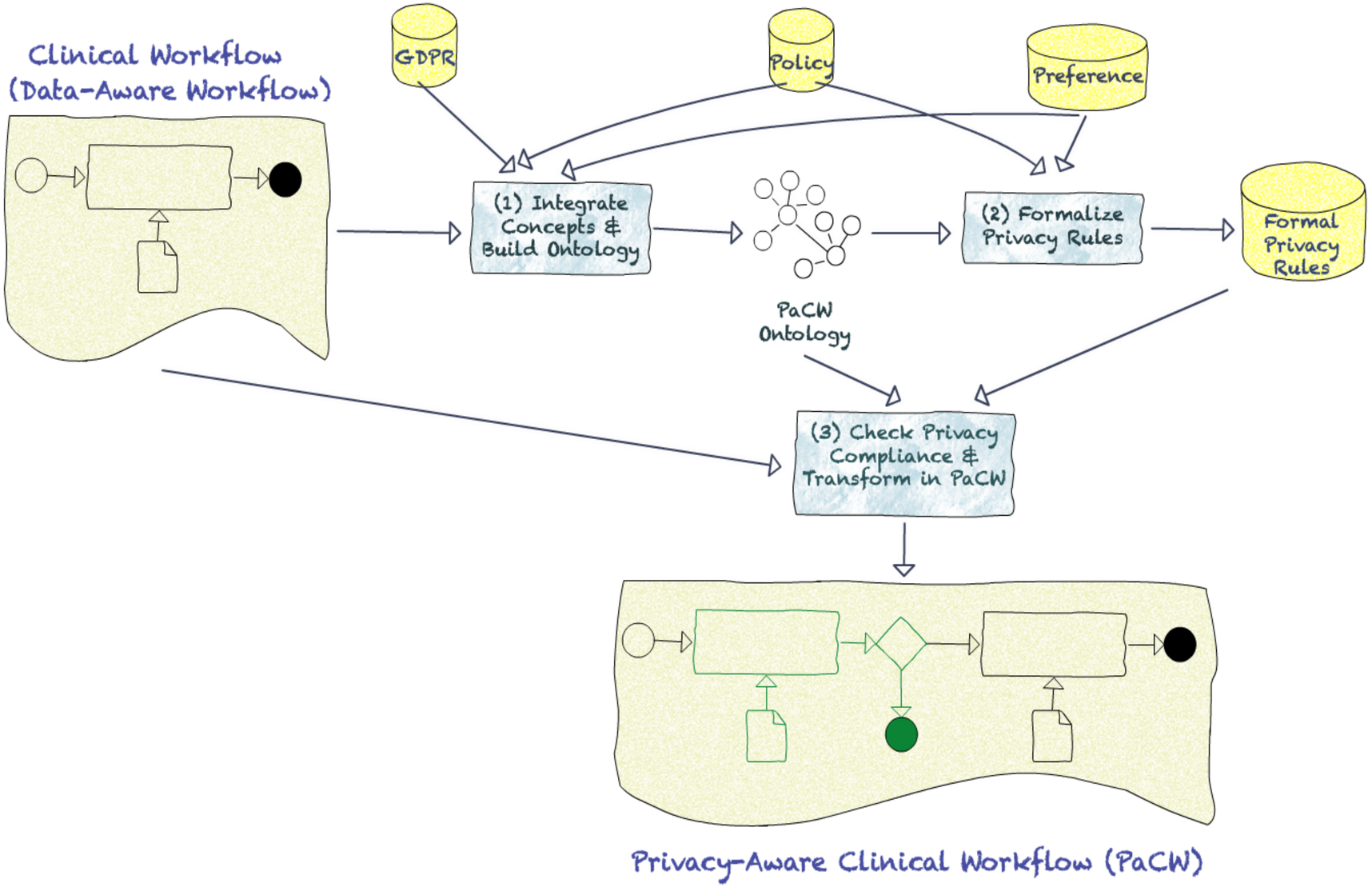
HEARING PROCEDURE - *AFTER TRANSFORMATION*

rule triggered due to performing hearing screening without consent check

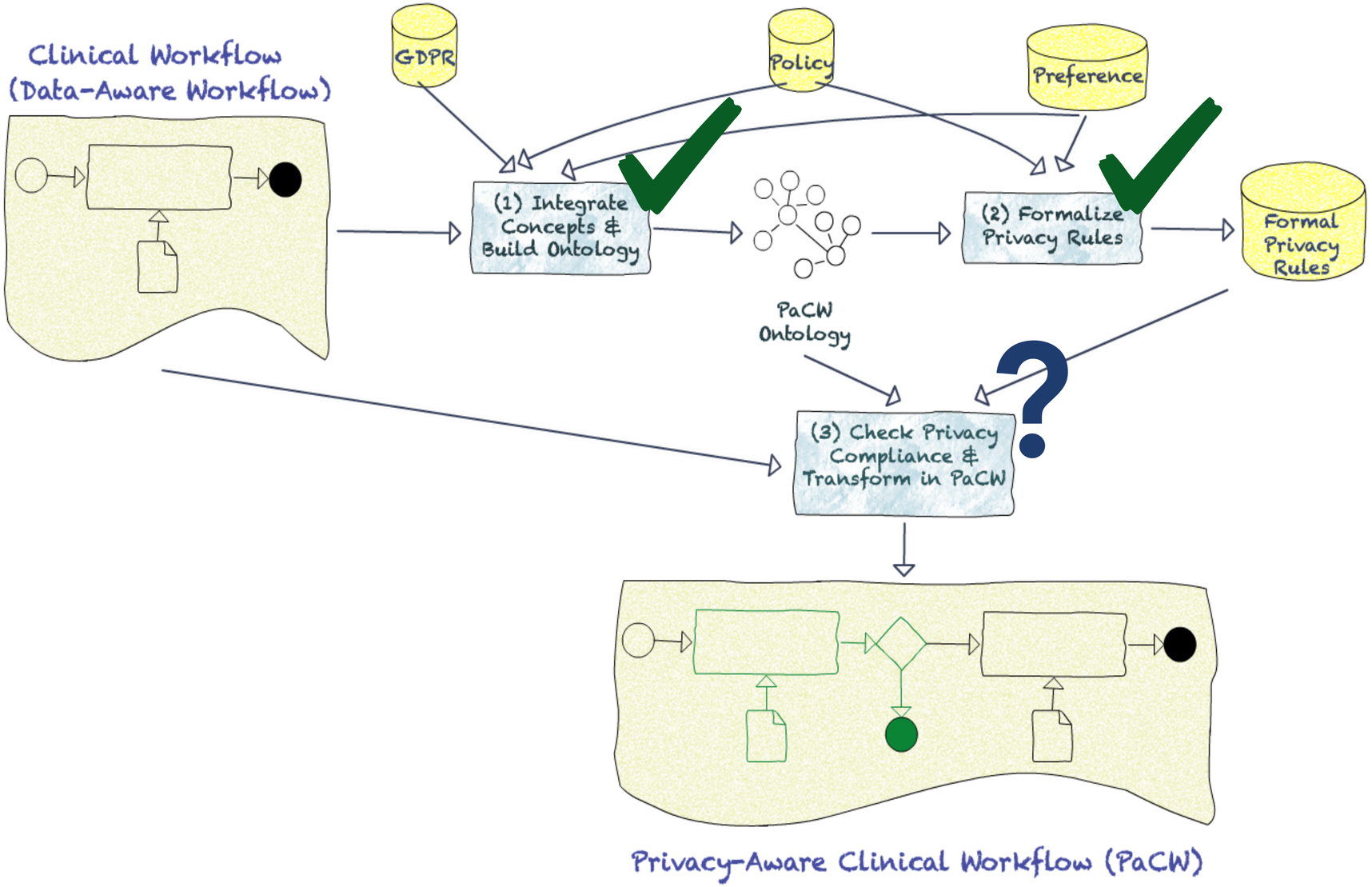
corrective action: add consent check pattern beforehand



SUMMARY


Clinical Workflow
(Data-Aware Workflow)
GDPR
Policy
Preference
(1) Integrate Concepts & Build Ontology
(2) Formalize Privacy Rules
Formal Privacy Rules
PaCW Ontology
(3) Check Privacy Compliance & Transform in PaCW
Privacy-Aware Clinical Workflow (PaCW)

SUMMARY


Clinical Workflow
(Data-Aware Workflow)
GDPR
Policy
Preference
(1) Integrate Concepts & Build Ontology
(2) Formalize Privacy Rules
Formal Privacy Rules
PaCW Ontology
(3) Check Privacy Compliance & Transform in PaCW
Privacy-Aware Clinical Workflow (PaCW)


MATT KENYON
THANK YOU! QUESTIONS??