Managing Consent in Workflows under GDPR

Saliha Irem BESIK
besiksal@informatik.hu-berlin.de
Supervisor: Prof. Johann-Christoph Freytag, Ph.D.

dbis
Institut für Informatik
Humboldt-Universität zu Berlin

Humboldt-Universität zu Berlin

Slides at https://irem.dev @irembesik

General Data Protection Regulation

- **data protection regulation** *for all individuals within European Union*
- *since* **25 May 2018**

General Data Protection Regulation

- **data protection regulation** *for all individuals within European Union*
- *since* **25 May 2018**

Goals

- **Protection:** *Protect* personal data
- **Control:** *Give* data subjects *control over* personal data

personal data: any information relating to an identifiable natural person ('data subject')

General Data Protection Regulation

- **data protection regulation** *for all individuals within European Union*
- *since* **25 May 2018**

Goals

- **Protection:** *Protect* personal data
- **Control:** *Give* data subjects *control over* personal data

- Organizations processing personal data must **comply with GDPR!**

personal data: any information relating to an identifiable natural person ('data subject')

GDPR Article 6 - *Lawfulness of processing*

- Processing of personal data must have **lawful basis**

GDPR Article 6 - *Lawfulness of processing*

- Processing of personal data must have **lawful basis**

Consent	Contract	Legal obligation
Vital Interest	Public Interest	Legitimate Interest

GDPR Article 6 - *Lawfulness of processing*

- Processing of personal data must have **lawful basis**

Consent	Contract	Legal obligation
Vital Interest	Public Interest	Legitimate Interest

GDPR Article 6 - *Lawfulness of processing*

- Processing of personal data must have **lawful basis**

Consent	Contract	Legal obligation
Vital Interest	Public Interest	Legitimate Interest

Processing shall be lawful […] if data subject has given consent to the processing of his personal data for one or more specific purposes

GDPR Article 6 - *Lawfulness of processing*

- Processing of personal data must have **lawful basis**

Consent	Contract	Legal obligation
Vital Interest	Public Interest	Legitimate Interest

Processing shall be lawful […] if data subject has given consent to the processing of his personal data for one or more specific purposes

purpose: the reason for which personal data is processed (e.g. marketing, treatment etc.)

CONSENT & REVOCATION UNDER GDPR

GDPR Article 4 §11 - *Definitions*

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

by which a data subject agrees to the processing of his / her personal data

CONSENT & REVOCATION UNDER GDPR

GDPR Article 4 §11 - *Definitions* → Valid Consent

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

by which a data subject agrees to the processing of his / her personal data

CONSENT & REVOCATION UNDER GDPR

GDPR Article 4 §11 - *Definitions* → Valid Consent

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

by which a data subject agrees to the processing of his / her personal data

GDPR Article 7 § 3 - *Conditions for consent*

The data subject have right to withdraw his / her consent at any time

CONSENT & REVOCATION UNDER GDPR

GDPR Article 4 §11 - *Definitions* → Valid Consent

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

by which a data subject agrees to the processing of his / her personal data

GDPR Article 7 § 3 - *Conditions for consent* → Revocation

The data subject have right to withdraw his / her consent at any time

OUTLINE

- Motivation: Privacy by Design via Workflows
- Research Problem
- Foundation
- Approach
- Summary § Outlook

OUTLINE

- **Motivation: Privacy by Design via Workflows**
- **Research Problem**
- Foundation
- Approach
- Summary § Outlook

MOTIVATION: PRIVACY BY DESIGN

GDPR says: Consider privacy at design phase…

MOTIVATION: PRIVACY BY DESIGN

GDPR says: Consider privacy at design phase…

Good News: Workflows might help!

MOTIVATION: PRIVACY BY DESIGN

GDPR says: Consider privacy at design phase…

Good News: Workflows might help!

A Workflow includes a series of tasks *to achieve a goal*

MOTIVATION: PRIVACY BY DESIGN

GDPR says: Consider privacy at design phase…

Good News: Workflows might help!

A Workflow includes a series of tasks *to achieve a goal*

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

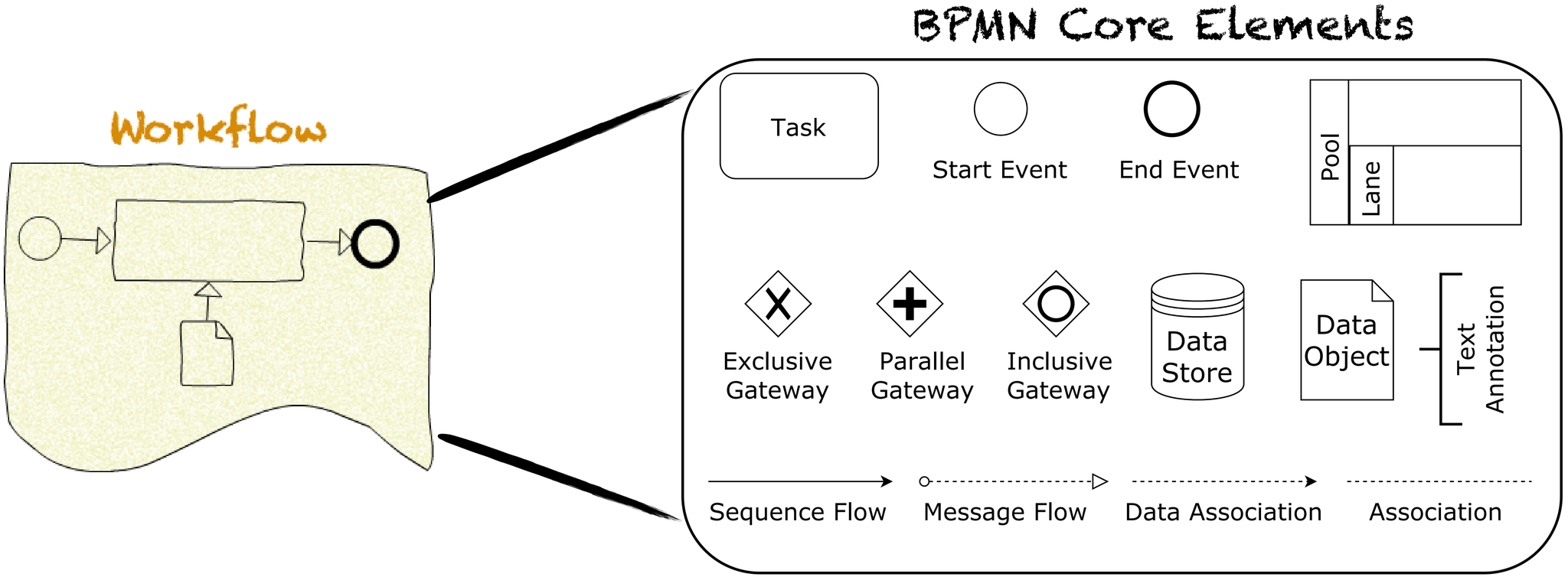
PRIVACY BY DESIGN VIA WORKFLOWS

PRIVACY BY DESIGN VIA WORKFLOWS

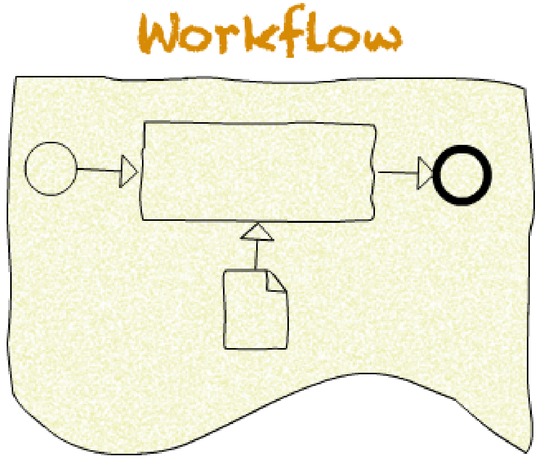
Workflow (Model) ≈ *Business Process Modeling Notation (BPMN) Model*

PRIVACY BY DESIGN VIA WORKFLOWS

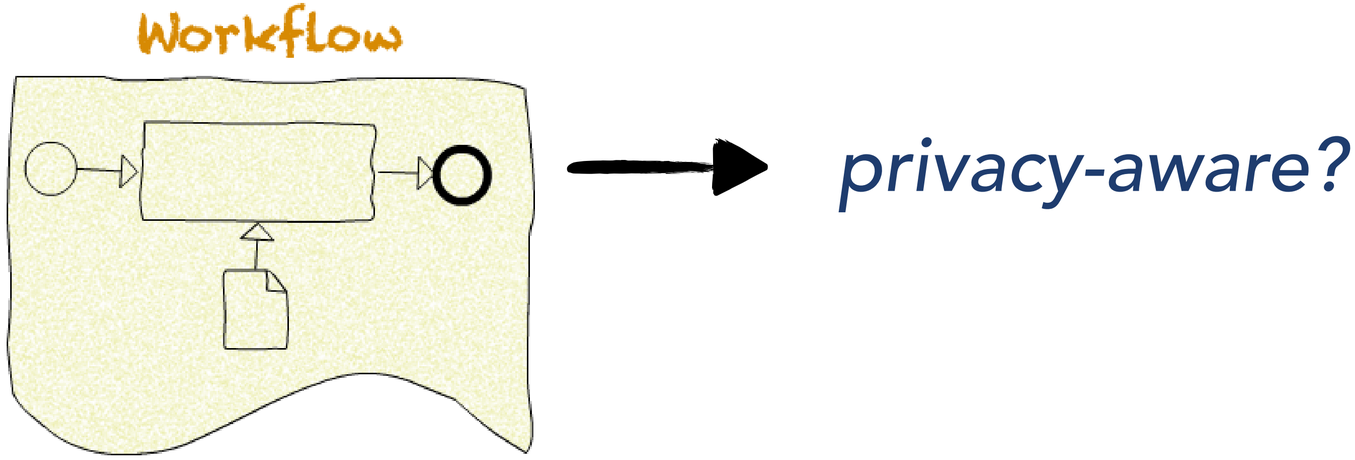
Workflow (Model) ≈ *Business Process Modeling Notation (BPMN) Model*



RESEARCH PROBLEM

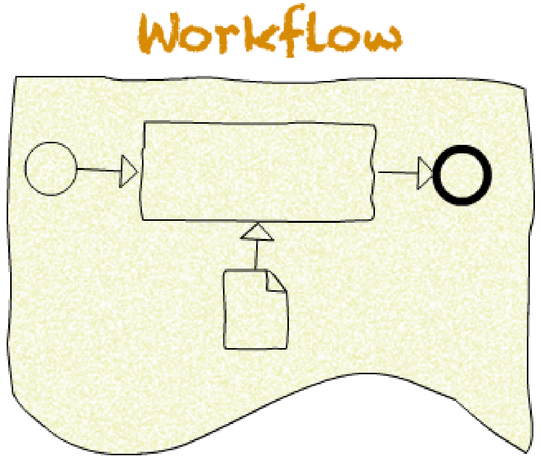


RESEARCH PROBLEM



privacy-aware?

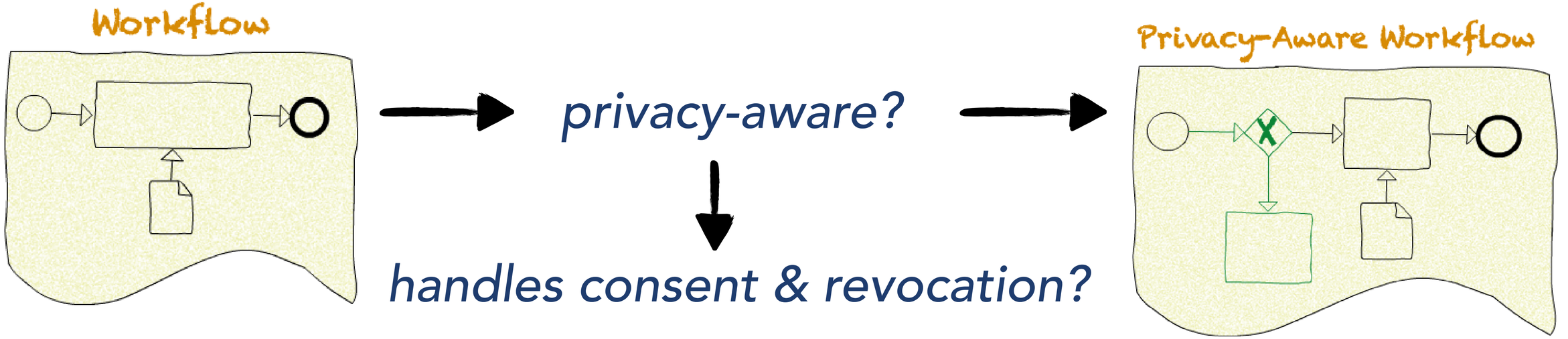
RESEARCH PROBLEM



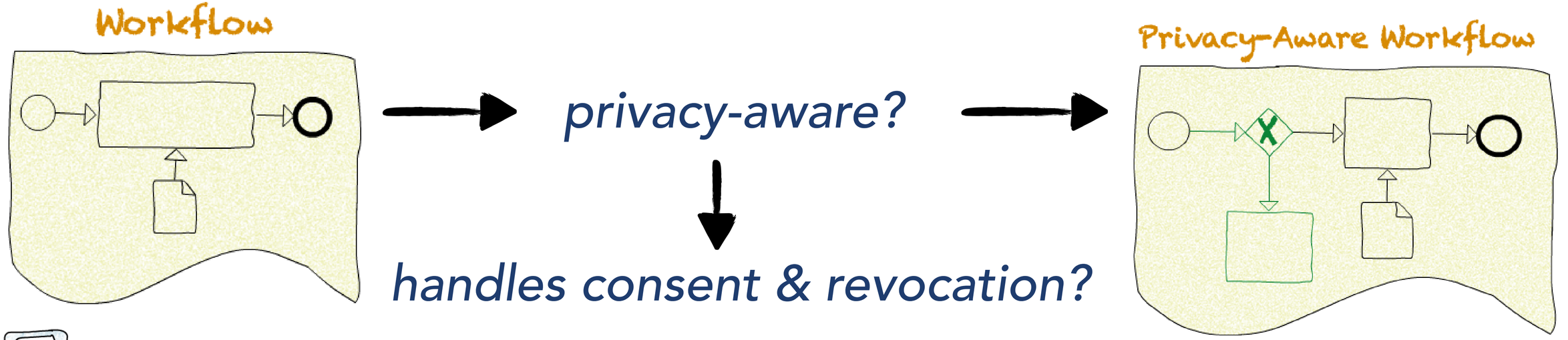
privacy-aware?

handles consent & revocation?

RESEARCH PROBLEM

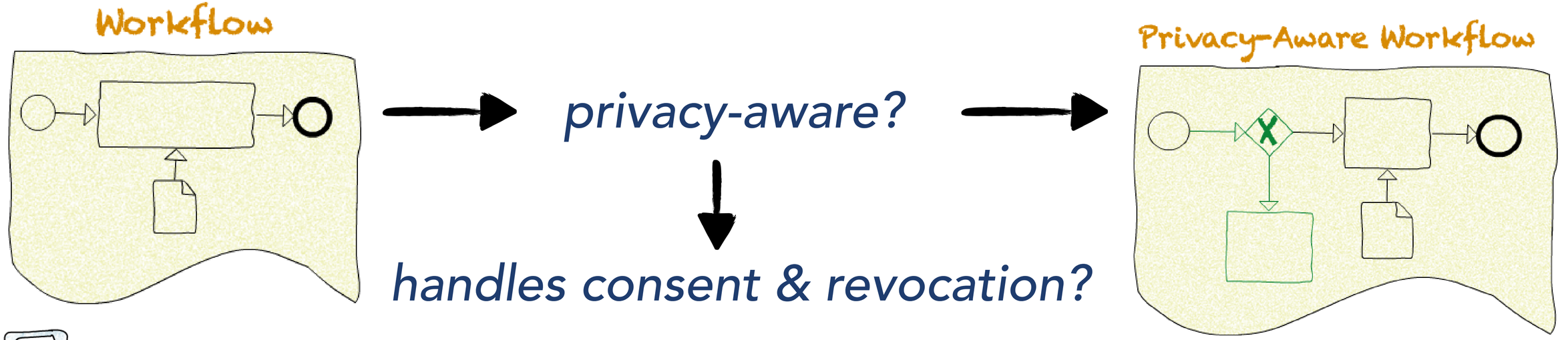


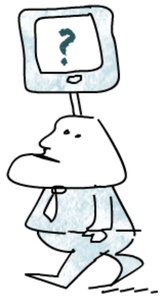
RESEARCH PROBLEM



How to **handle consent?**

RESEARCH PROBLEM

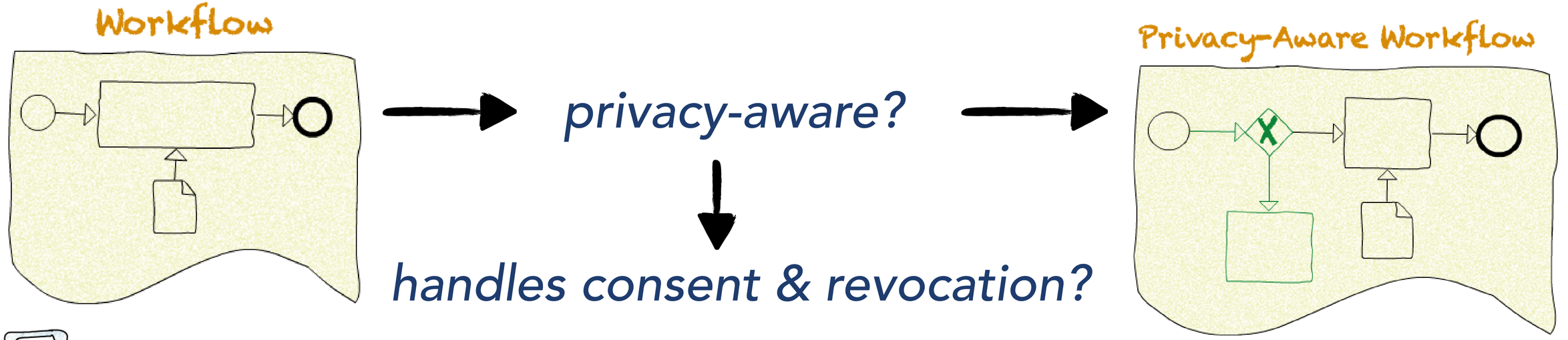




How to **handle consent?**

How to **handle revocation?**

RESEARCH PROBLEM



How to **handle consent?**

How to **handle revocation?**

Approach: Design Patterns

OUTLINE

- Motivation
- Research Problem
- **Foundation**
  - **Data-Aware Workflow** 
  - **Consent Policy** 
  - **Consent Form** 
- Approach
- Summary § Outlook

FOUNDATION

Which sources needed to handle consent ?

FOUNDATION

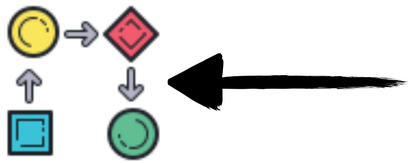
Which sources needed to handle consent ?

1- **Data-Aware Workflow**

FOUNDATION

Which sources needed to handle consent ?

1- **Data-Aware Workflow**



Which *data attributes* are (potentially) used for which *purpose* in the Workflow

FOUNDATION

Which sources needed to handle consent ?

1- **Data-Aware Workflow**

Which *data attributes* are (potentially) used for which *purpose* in the Workflow

2- **Consent Policy**

FOUNDATION

Which sources needed to handle consent ?

1- **Data-Aware Workflow**

Which *data attributes* are (potentially) used for which *purpose* in the Workflow

2- **Consent Policy**

Which *purposes* require consent to be lawful

FOUNDATION

Which sources needed to handle consent ?

1- **Data-Aware Workflow** 

Which *data attributes* are (potentially) used for which *purpose* in the Workflow

2- **Consent Policy** 

Which *purposes* require consent to be lawful

3- **Consent Form** 

FOUNDATION

Which sources needed to handle consent ?

1- **Data-Aware Workflow** 

Which *data attributes* are (potentially) used for which *purpose* in the Workflow

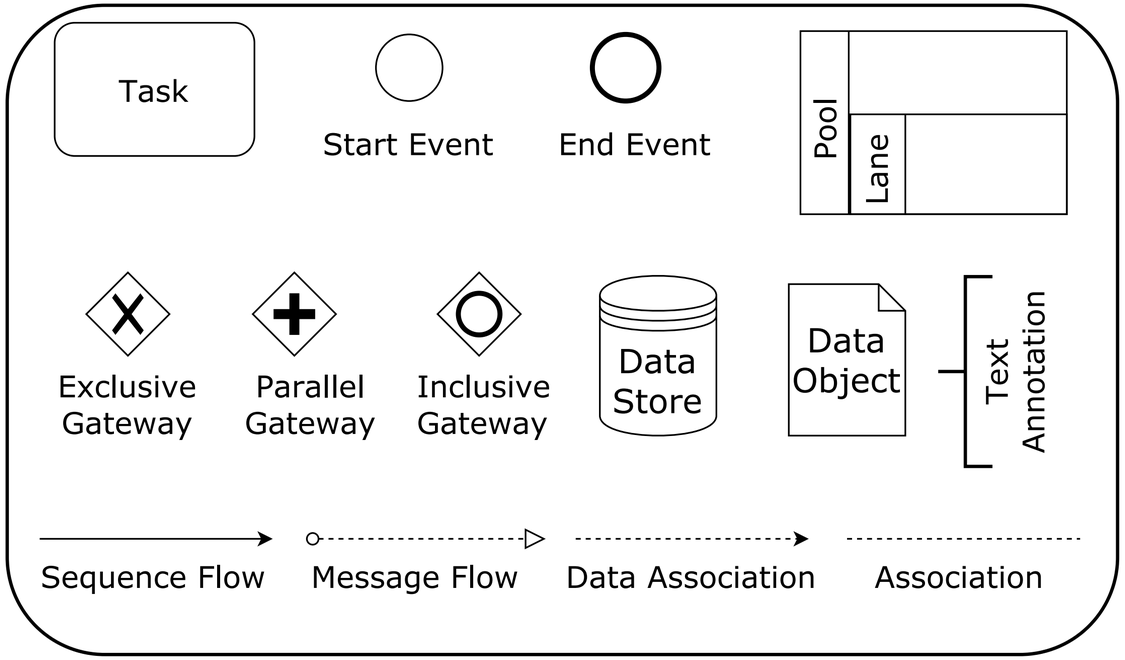
2- **Consent Policy** 

Which *purposes* require consent to be lawful

3- **Consent Form** 

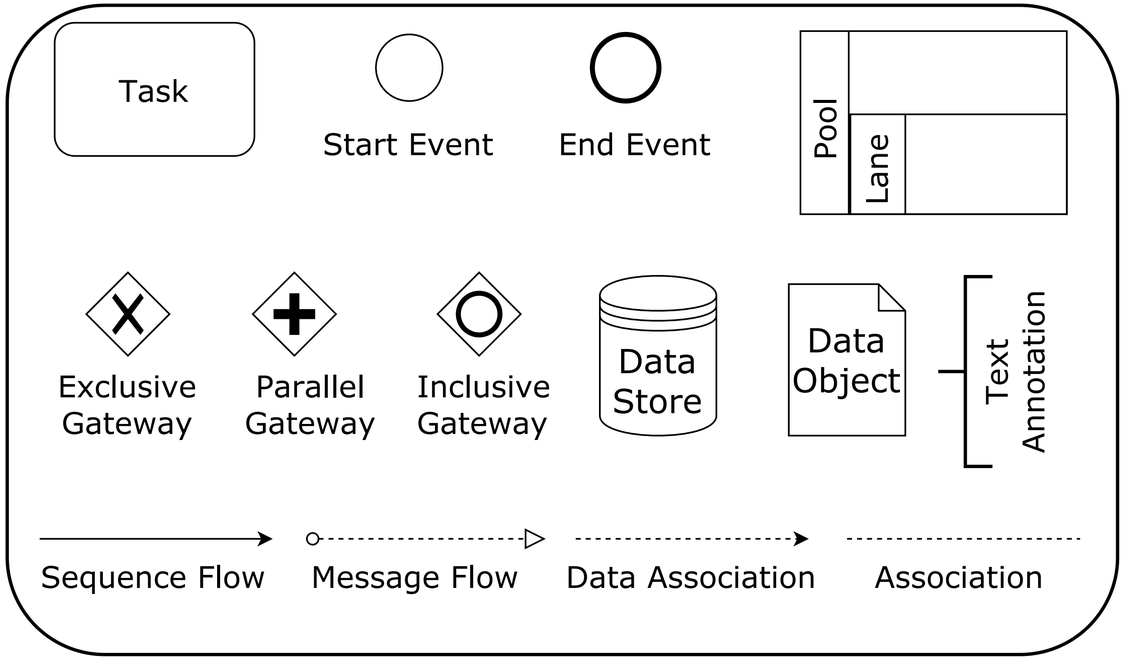
Which *information* should be given to data subject for a valid consent

Workflow



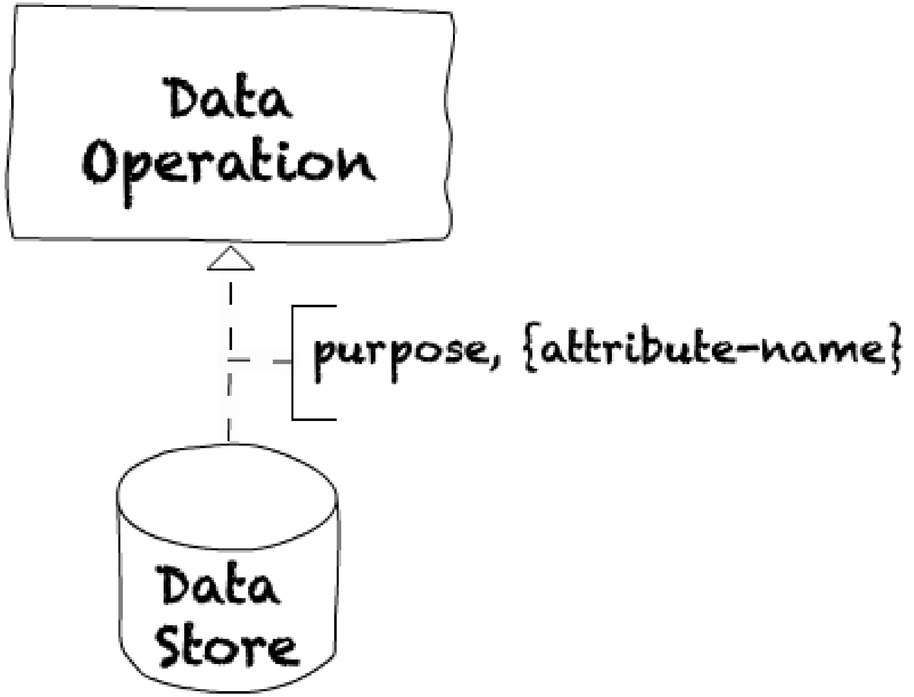
BPMN Core Elements

Workflow → Data-Aware Workflow

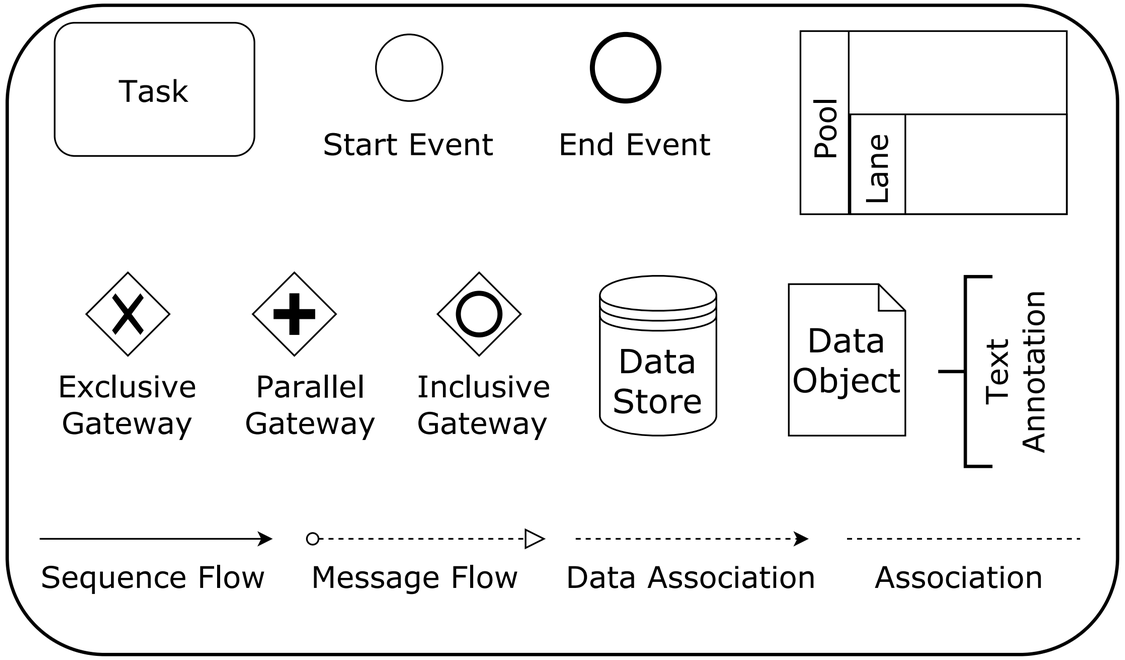


BPMN Core Elements

+

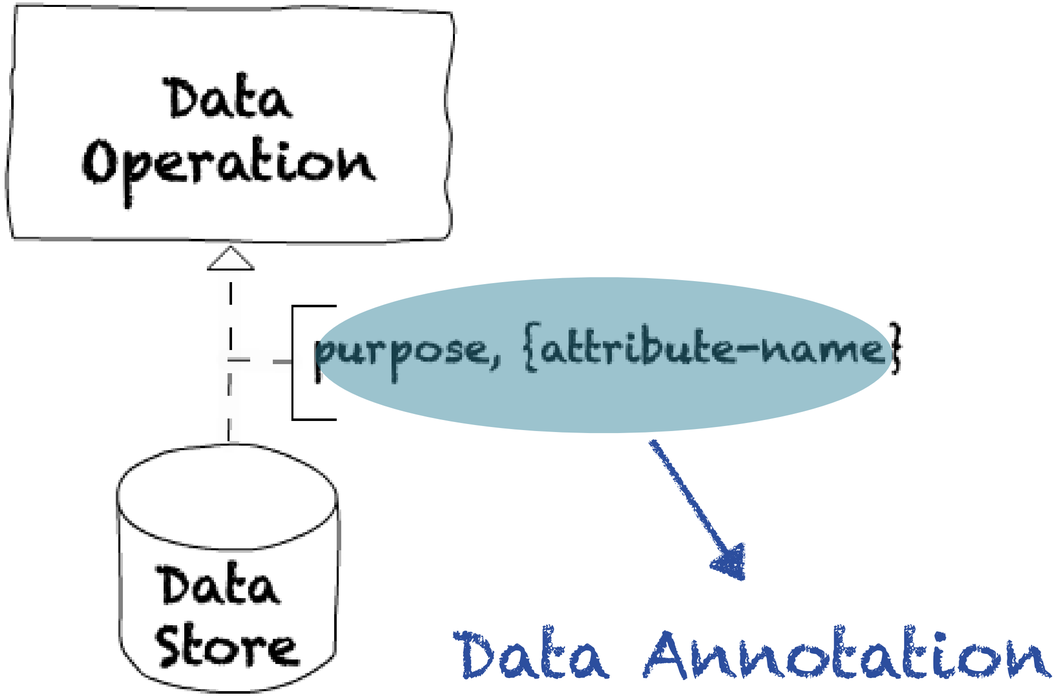


Workflow → Data-Aware Workflow



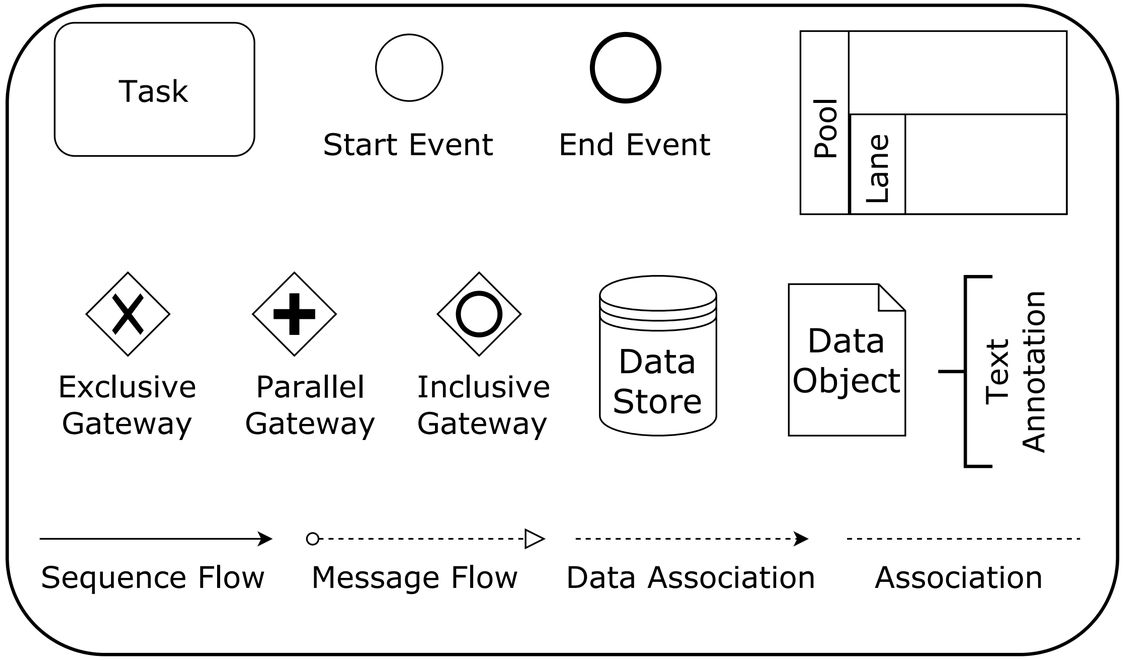
BPMN Core Elements

+



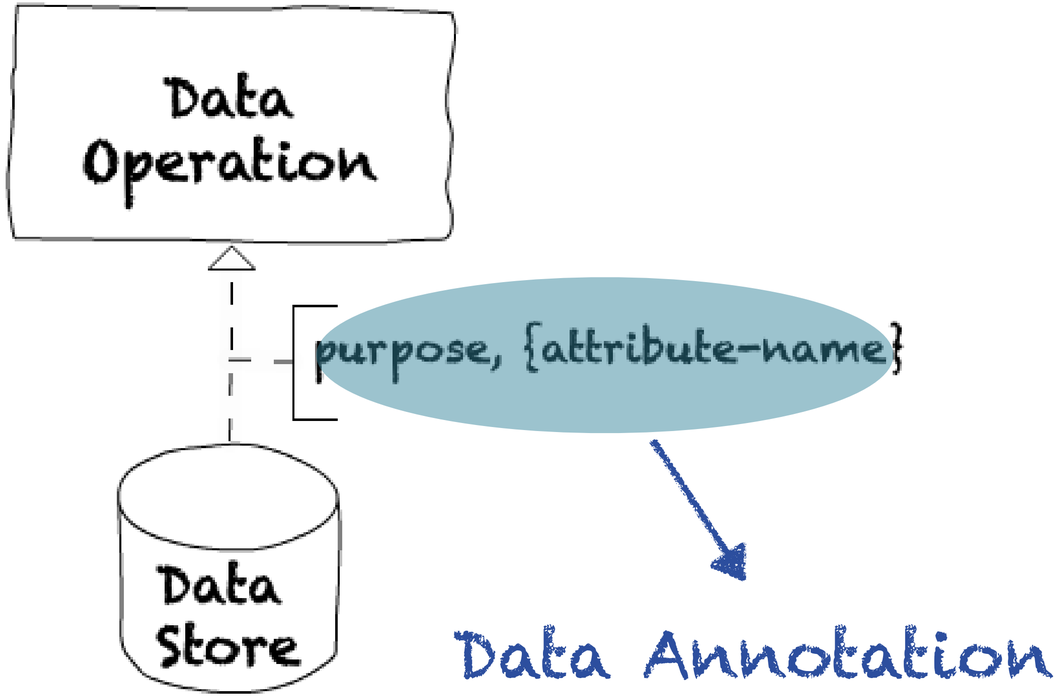
Data Annotation

Workflow → Data-Aware Workflow



BPMN Core Elements

+



** Different types of Data Handling in BPMN are stated in [1]*

[1] Besik, Saliha Irem, and Johann-Christoph Freytag. "Ontology-Based Privacy Compliance Checking for Clinical Workflows."

CONSENT POLICY

- the modality of data processing, obligatory or voluntary (requires consent)

CONSENT POLICY

- the modality of data processing, obligatory or voluntary (requires consent)

A consent 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}*

CONSENT POLICY

- the modality of data processing, obligatory or voluntary (requires consent)

A consent 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.

CONSENT POLICY

- the modality of data processing, obligatory or voluntary (requires consent)

A consent 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.

CONSENT POLICY

- the modality of data processing, obligatory or voluntary (requires consent)

A consent 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 ?

CONSENT POLICY

- the modality of data processing, obligatory or voluntary (requires consent)

A consent 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 ?

CONSENT POLICY

- the modality of data processing, obligatory or voluntary (requires consent)

A consent 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.

CONSENT POLICY

- the modality of data processing, obligatory or voluntary (requires consent)

A consent 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 ?

(newborn-hearing-screening, true)

CONSENT FORM

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

CONSENT FORM

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

CONSENT FORM

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

Valid consent

▸ Data Controller	
▸ Purpose	

Data Controller: natural person who determines the purposes and means of the processing

CONSENT FORM

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

Valid consent

▸ Data Controller	
▸ Purpose	

Example: We, as Hospital X, use your personal data for newborn hearing screening.

Data Controller: natural person who determines the purposes and means of the processing

CONSENT FORM

"any **freely given, specific, informed and unambiguous** [...] clear affirmative action"

Valid consent

Data Controller	Hospital X
Purpose	

Example: We, as Hospital X, use your personal data for newborn hearing screening.

Data Controller: natural person who determines the purposes and means of the processing

CONSENT FORM

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

Valid consent

Data Controller	Hospital X
Purpose	newborn hearing screening

Example: We, as Hospital X, use your personal data for newborn hearing screening.

Data Controller: natural person who determines the purposes and means of the processing

CONSENT FORM

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

Valid consent

Data Controller	Hospital X
Purpose	newborn hearing screening

Example: We, as Hospital X, use your personal data for newborn hearing screening.

When multiple purposes, consent should be given for all!

Data Controller: natural person who determines the purposes and means of the processing

CONSENT FORM

"any **freely given, specific, informed and unambiguous** […] clear affirmative action"

Valid consent

Data Controller	Hospital X
Purpose	newborn hearing screening

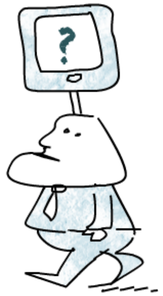
Example: We, as Hospital X, use your personal data for newborn hearing screening.

When multiple purposes, consent should be given for all! → Separate / Aggregated Consent Forms

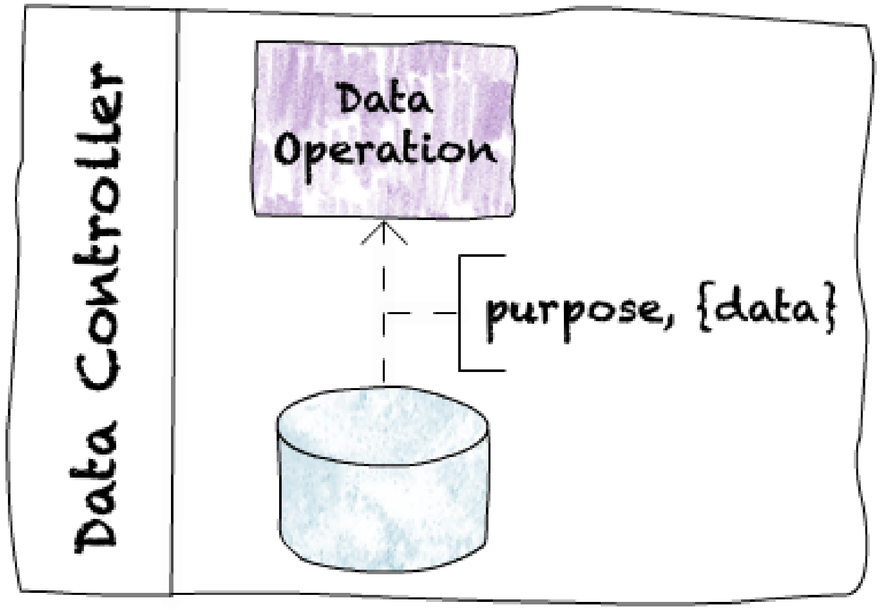
Data Controller: natural person who determines the purposes and means of the processing

OUTLINE

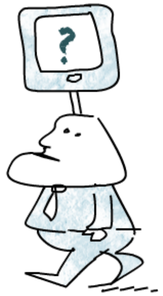
- Motivation
- Research Problem
- Foundation
- **Approach**
  - **Consent Pattern**
  - **Revocation Pattern**
  - **Examples**
- Summary § Outlook



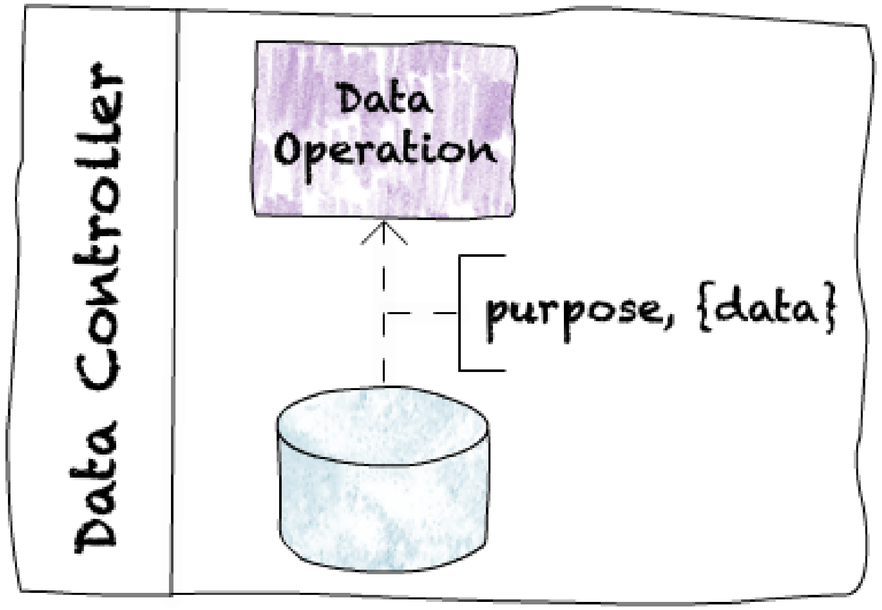
How to handle consent?



Policy: purpose requires consent 

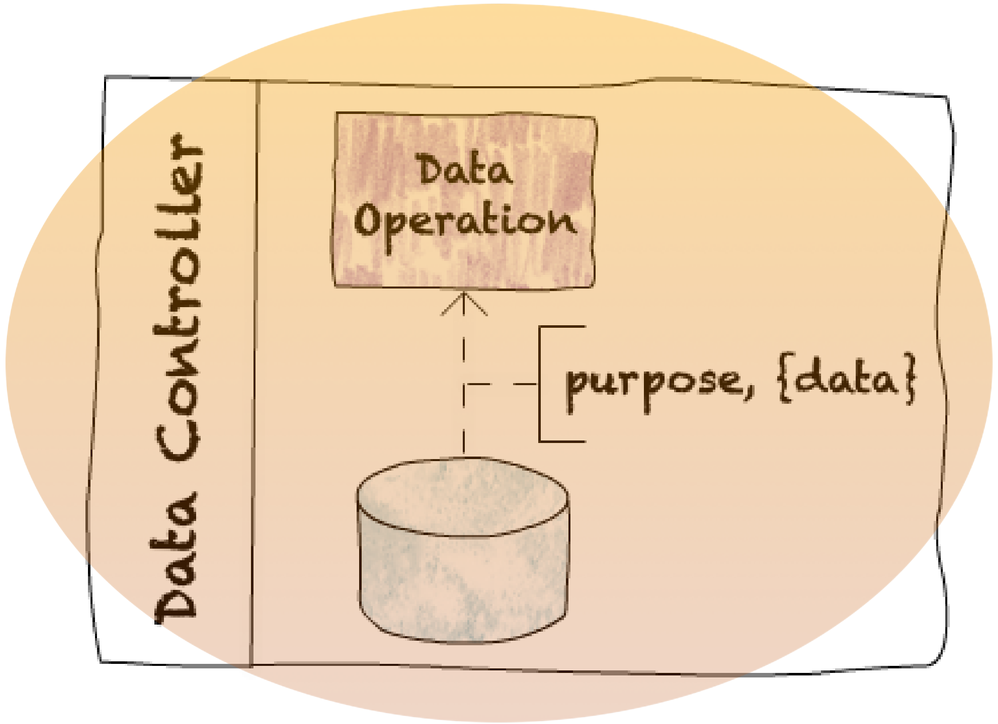


How to handle consent? → Consent Pattern



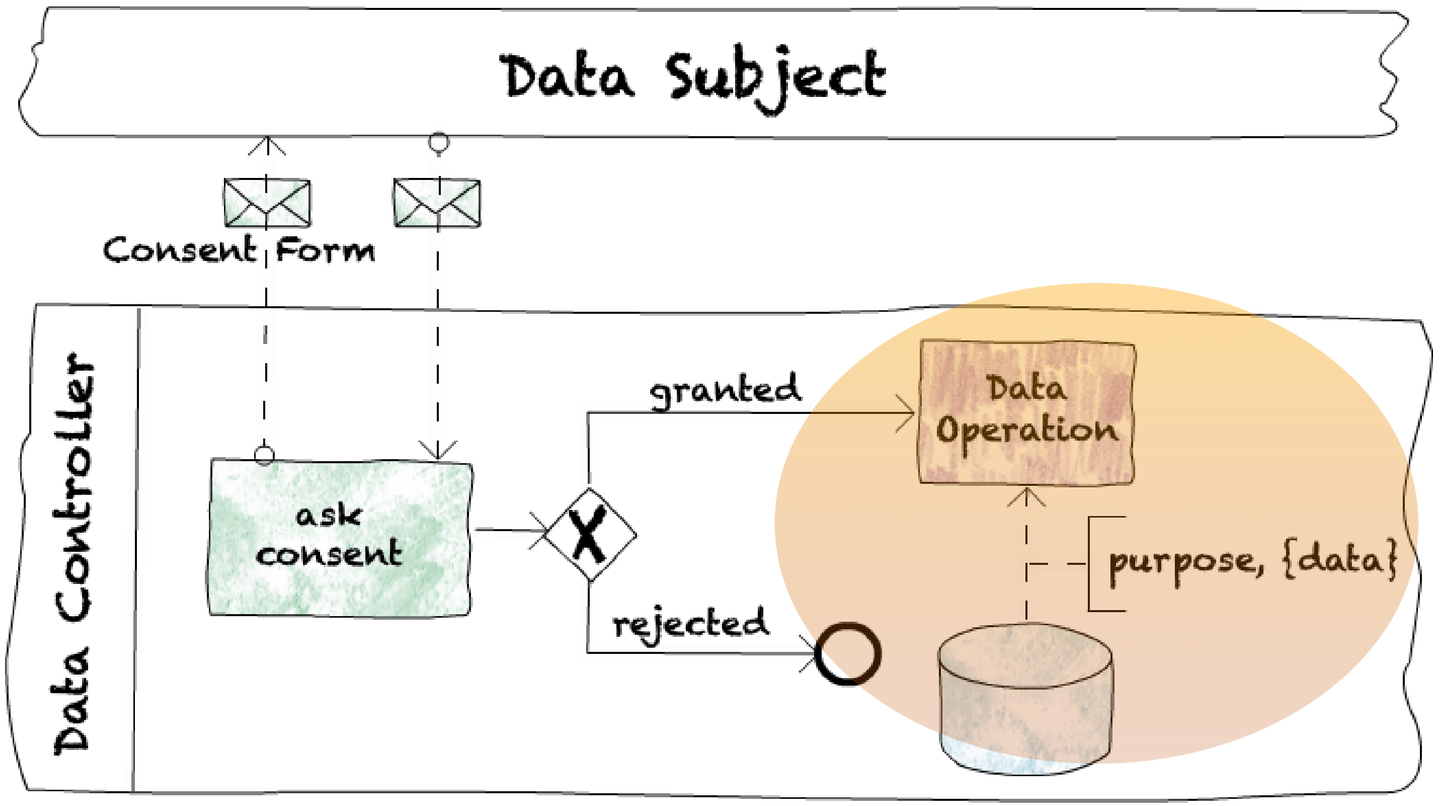
Policy: purpose requires consent

How to handle consent? → Consent Pattern



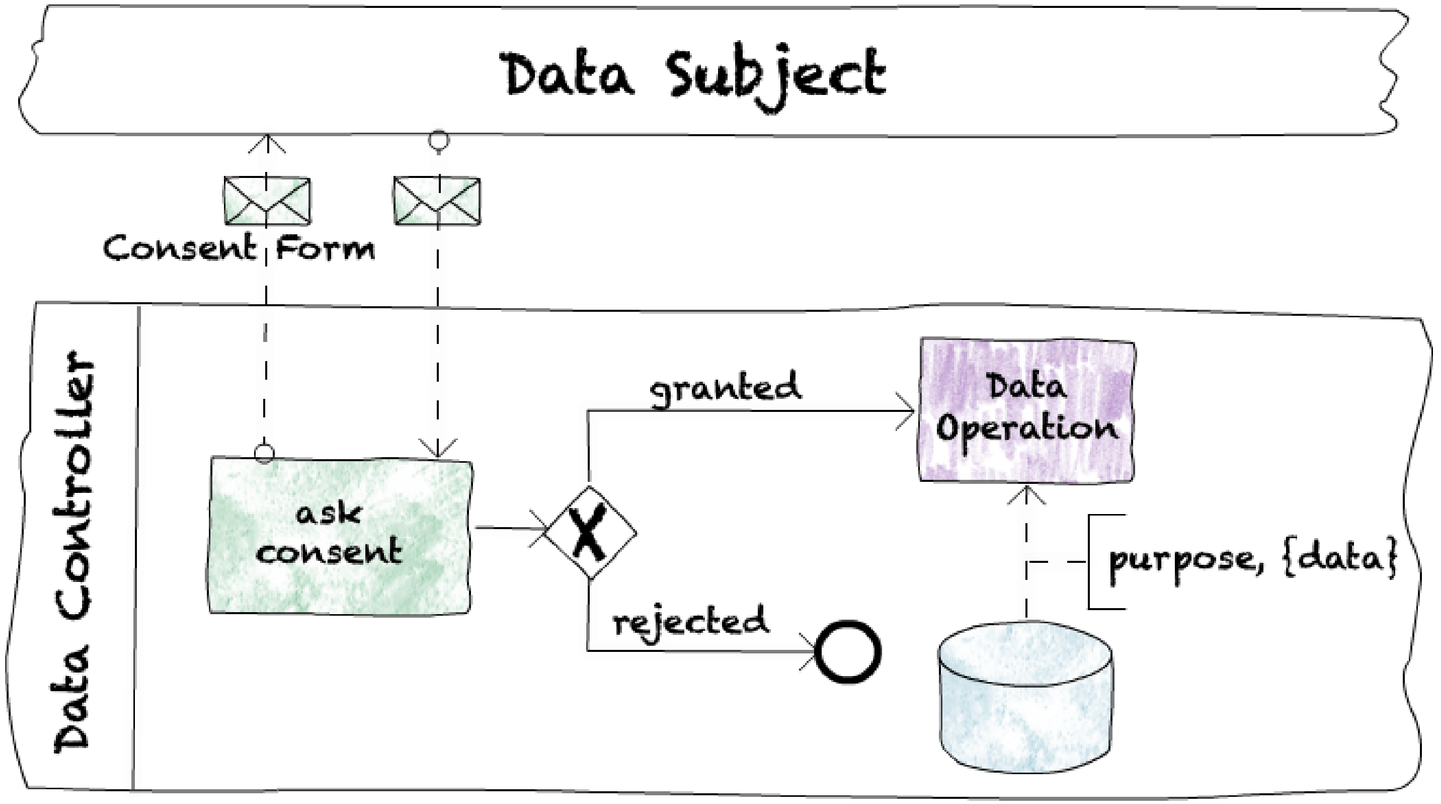
Policy: purpose requires consent

How to handle consent? → Consent Pattern

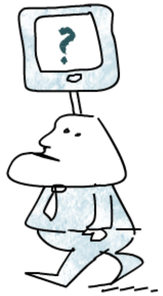


Policy: purpose requires consent

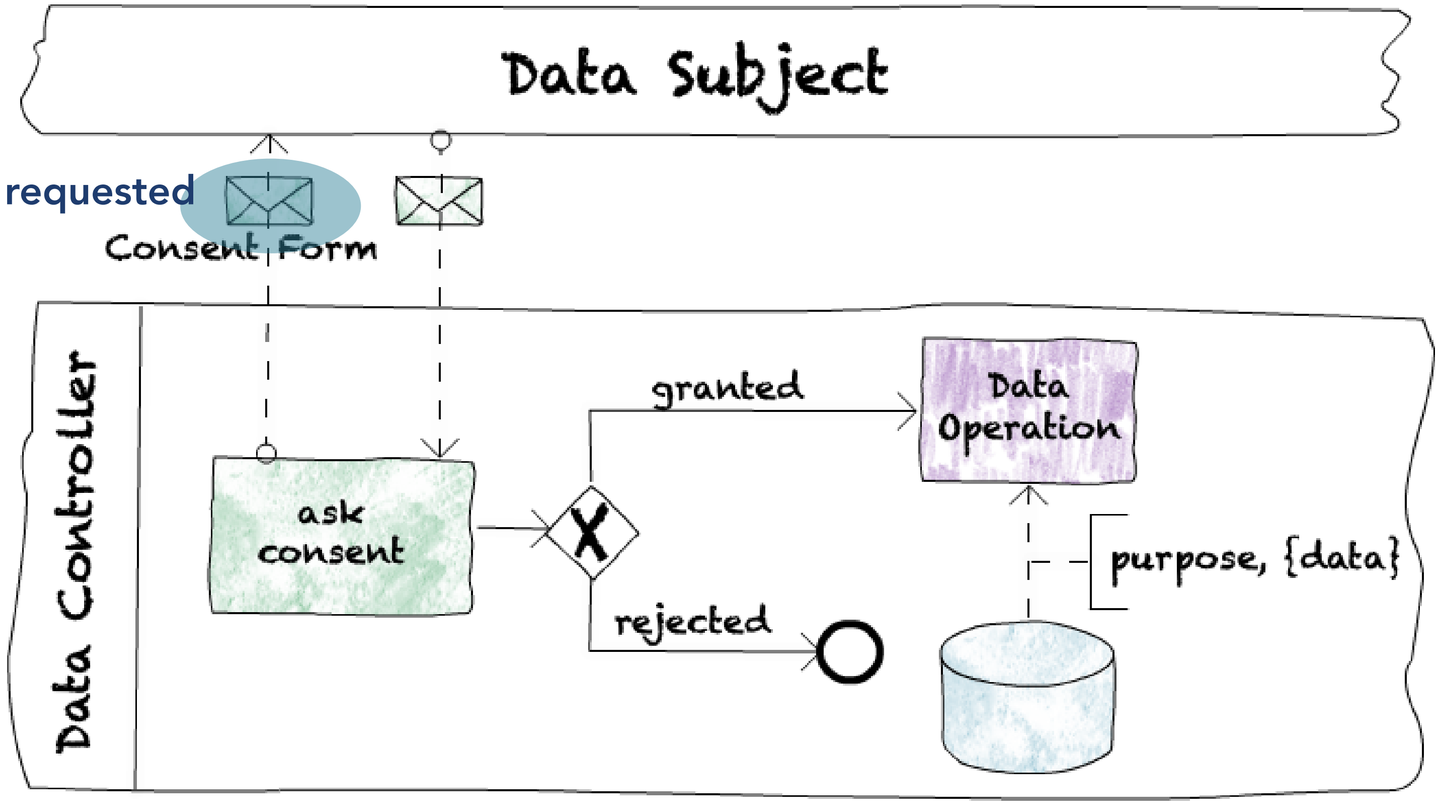
How to handle consent? → Consent Pattern



Policy: purpose requires consent

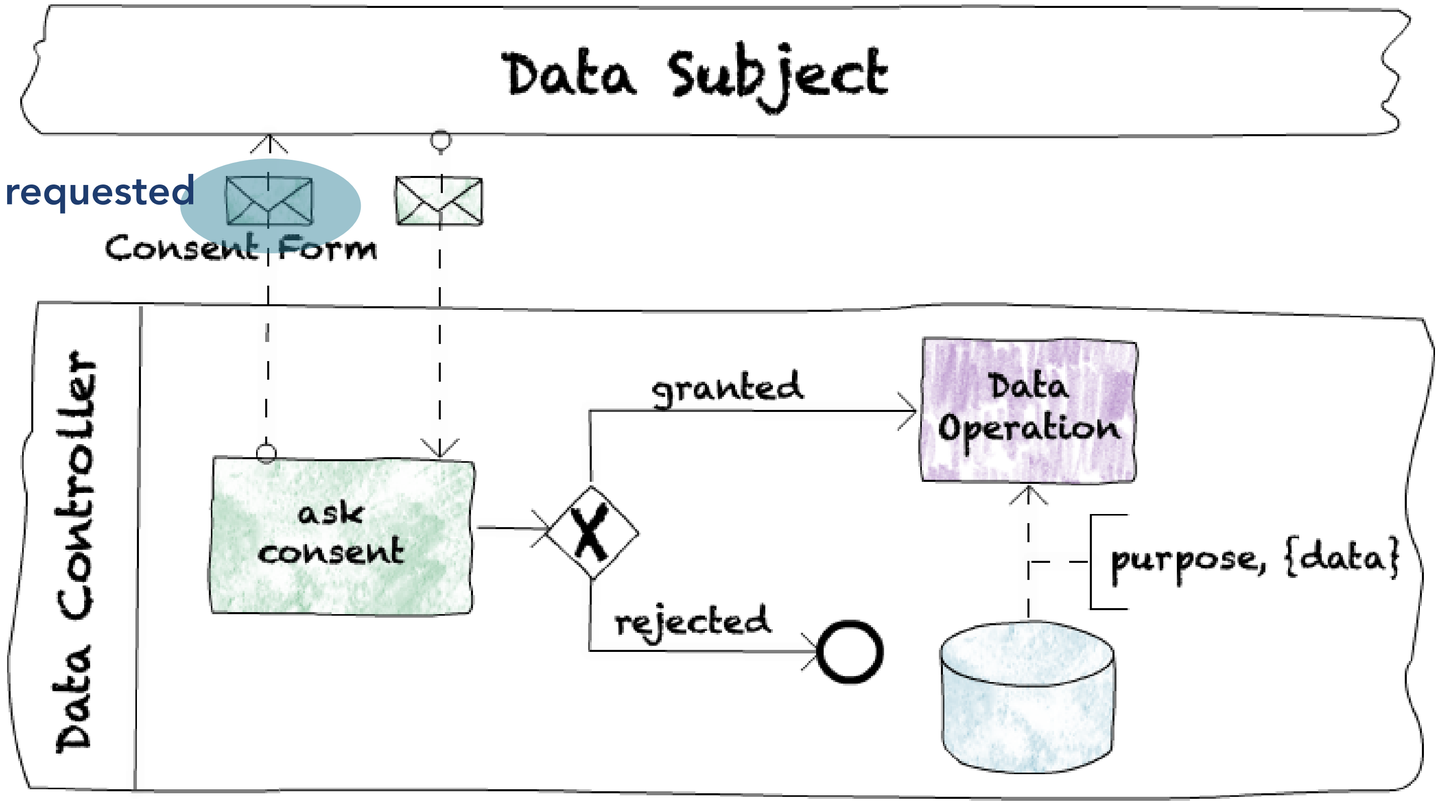


How to handle consent? → Consent Pattern



Policy: purpose requires consent

How to handle consent? → Consent Pattern



Consent Form

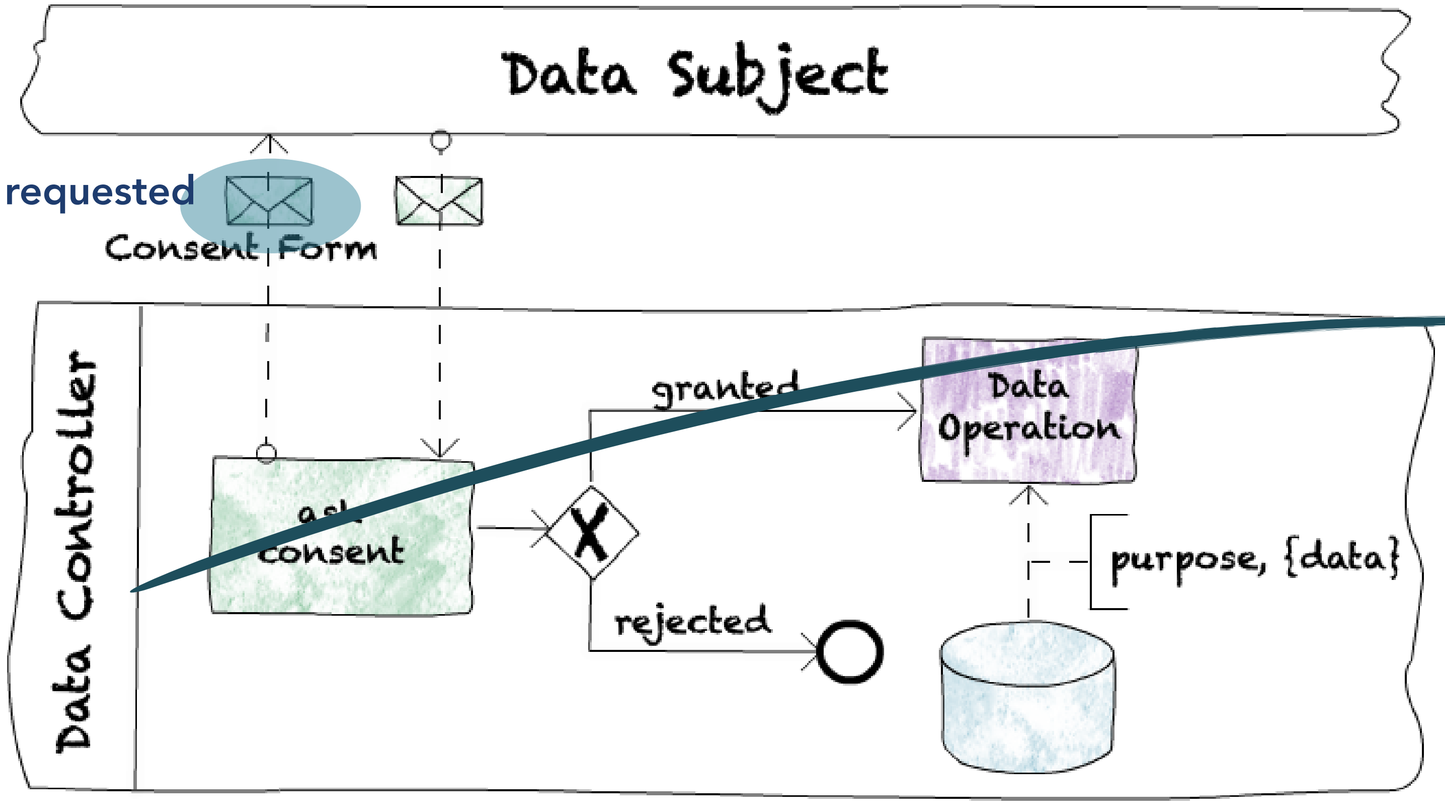
Data Controller

Purpose

Data Subject

Policy: purpose requires consent

How to handle consent? → Consent Pattern

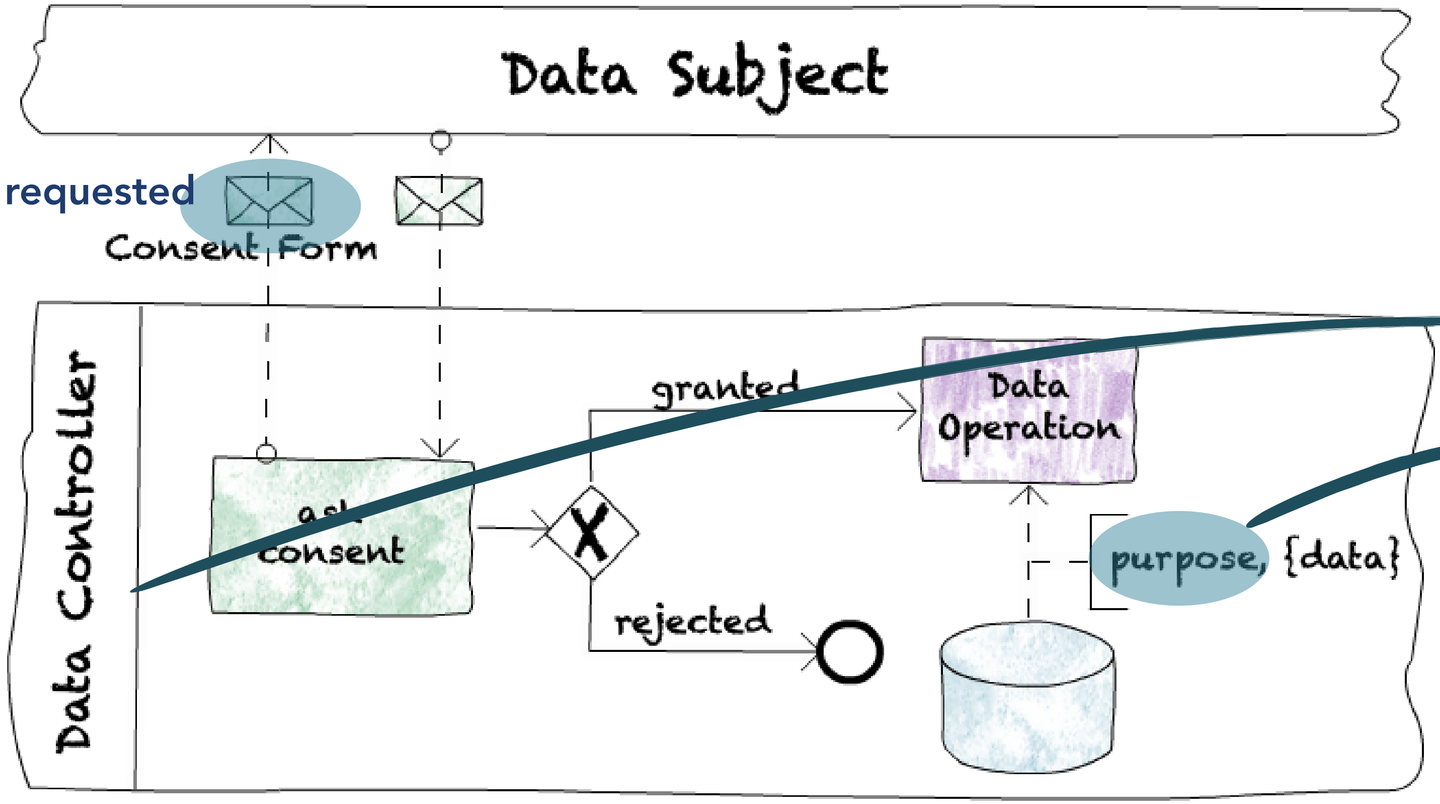


Consent Form

- Data Controller
- Purpose
- Data Subject

Policy: purpose requires consent

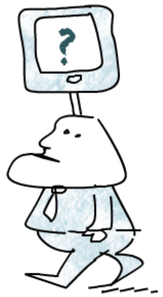
How to handle consent? → Consent Pattern



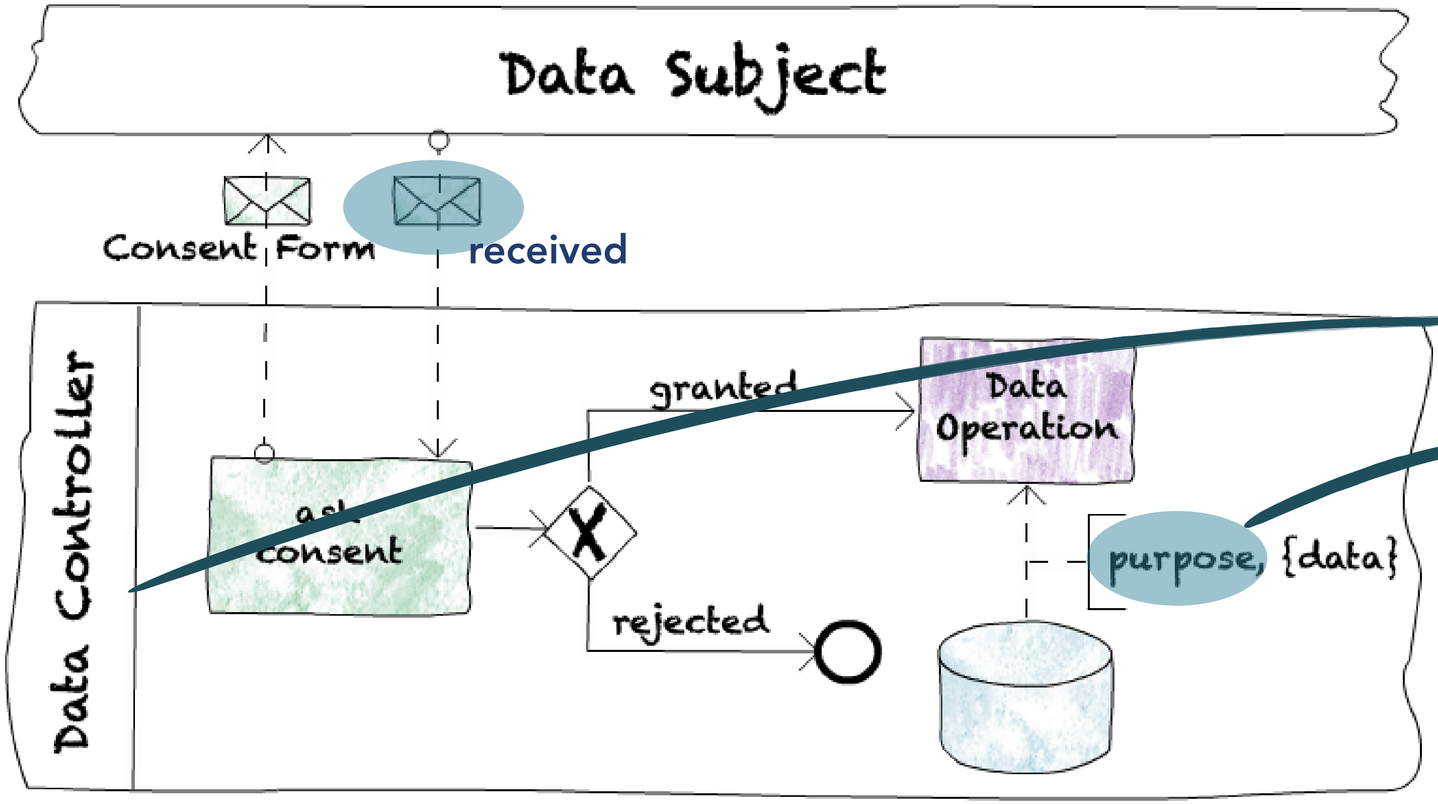
Consent Form

- Data Controller
- Purpose
- Data Subject

Policy: purpose requires consent



How to handle consent? → Consent Pattern

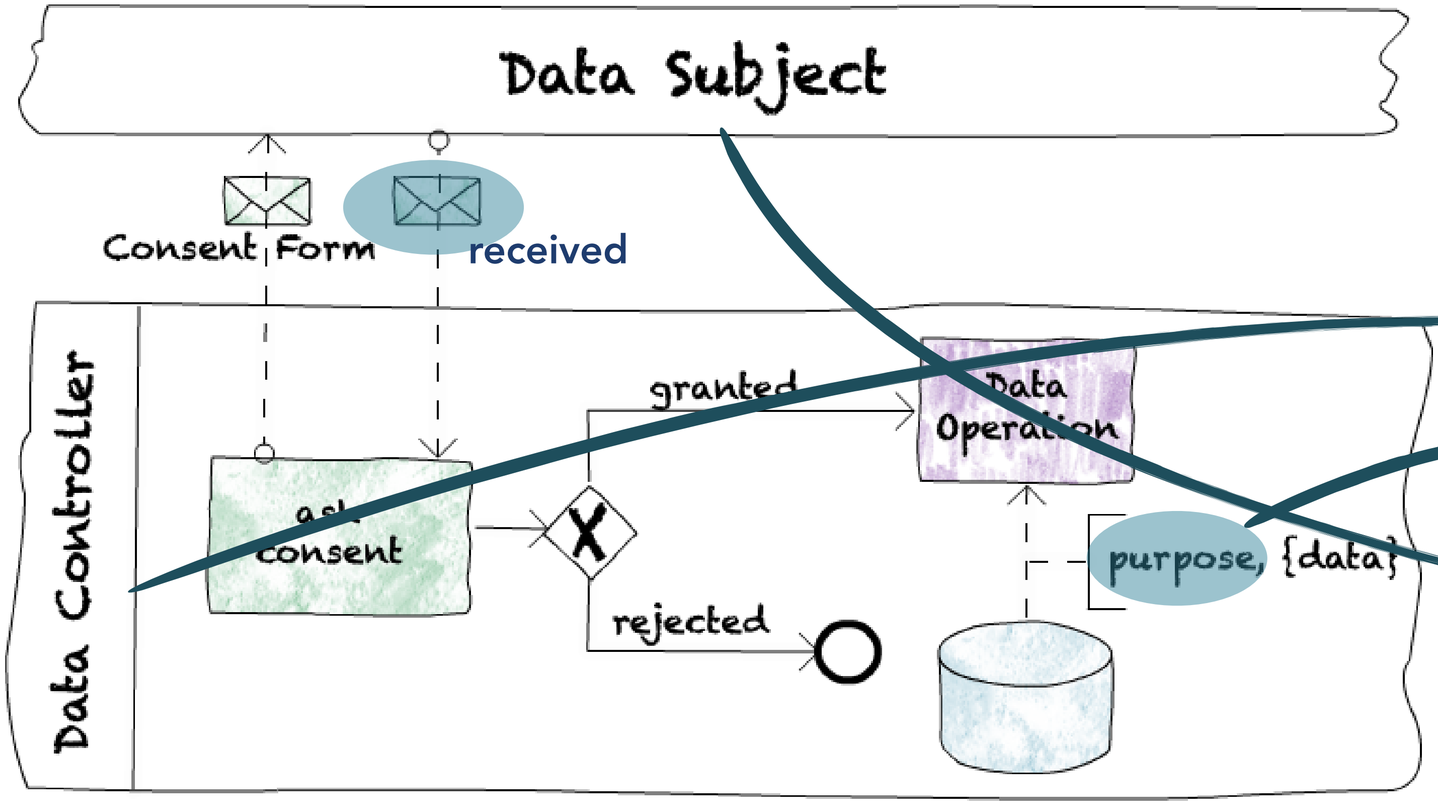


Consent Form

- Data Controller
- Purpose
- Data Subject

Policy: purpose requires consent

How to handle consent? → Consent Pattern

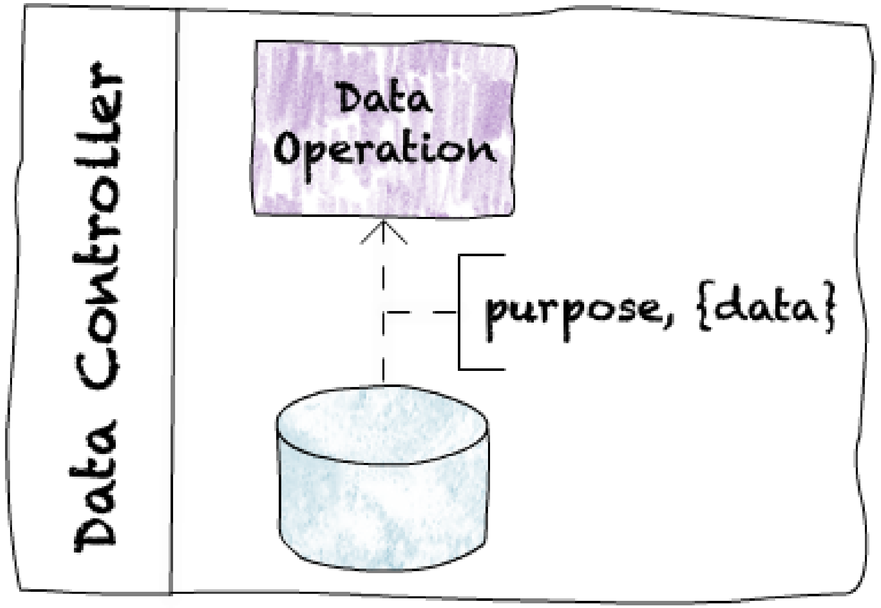


Consent Form

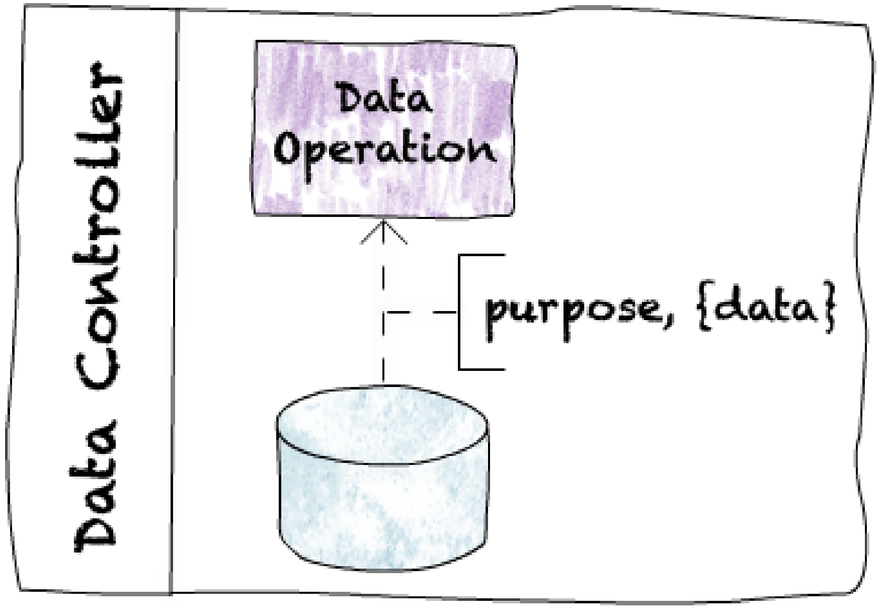
- Data Controller
- Purpose
- Data Subject

Policy: purpose requires consent

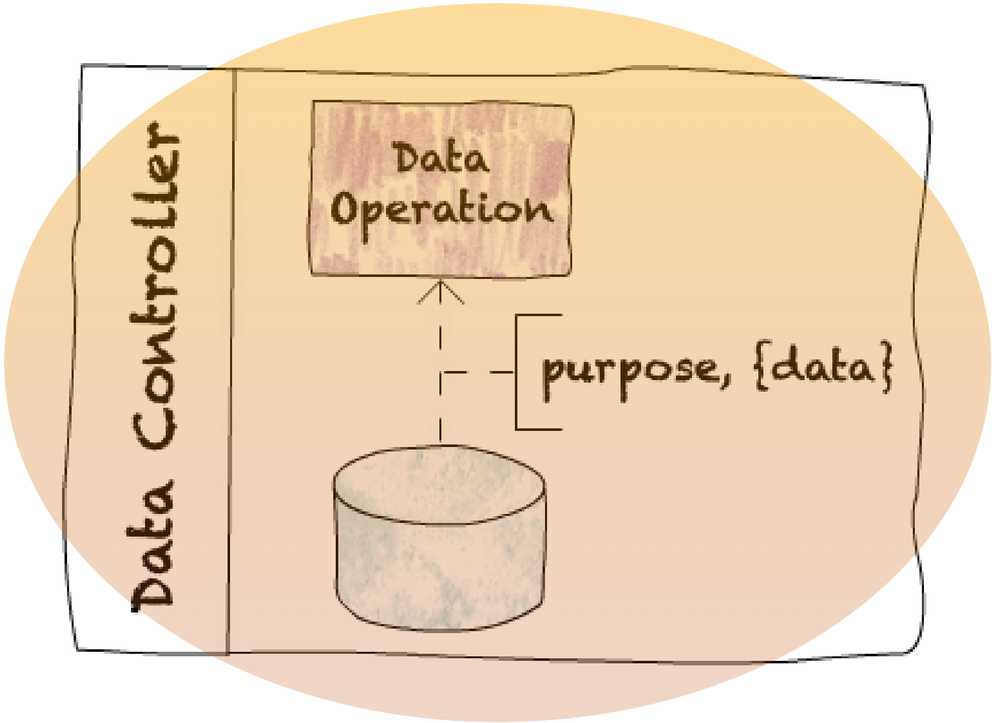
How to handle revocation?



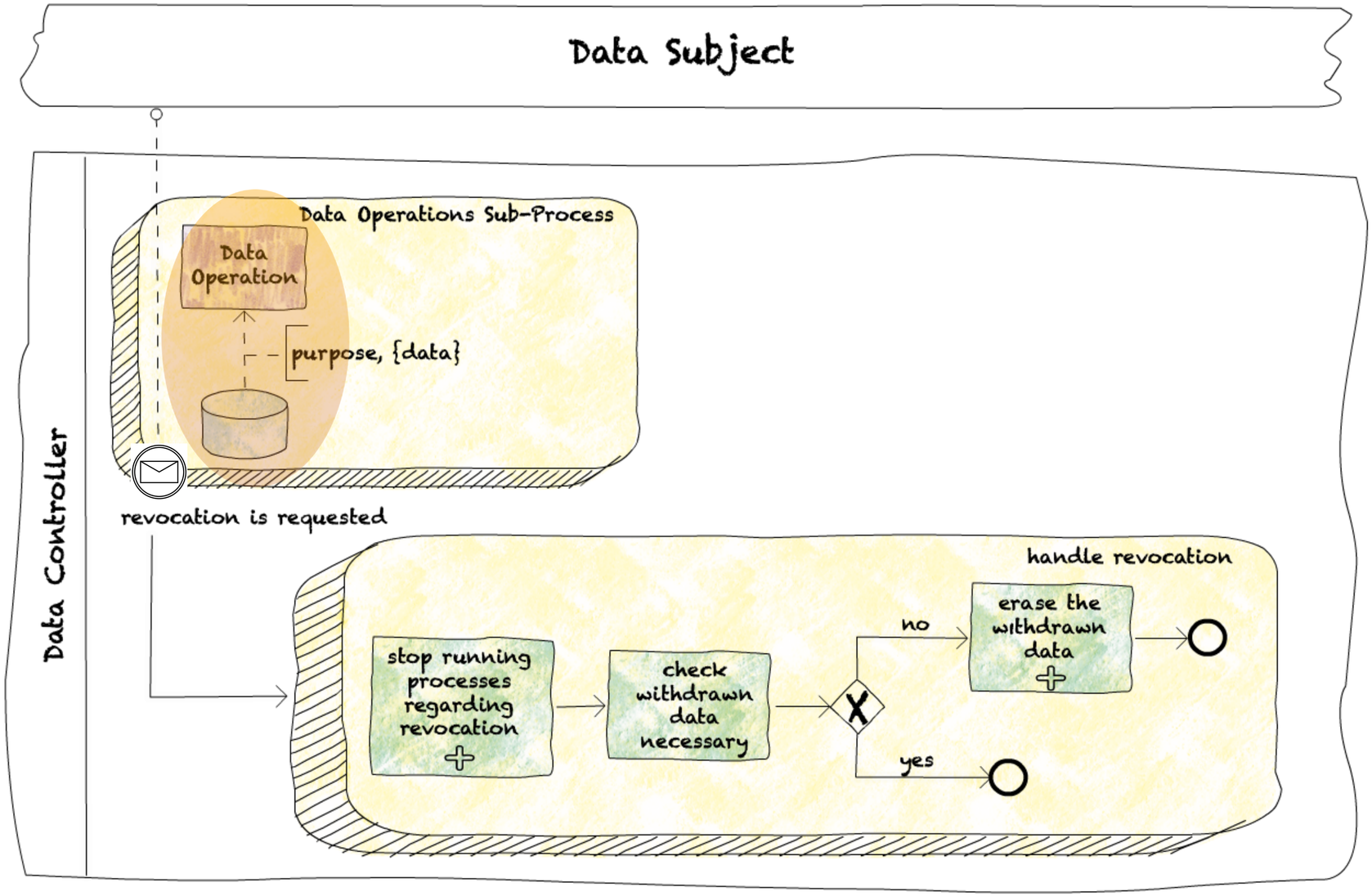
How to handle revocation? → **Revocation Pattern**



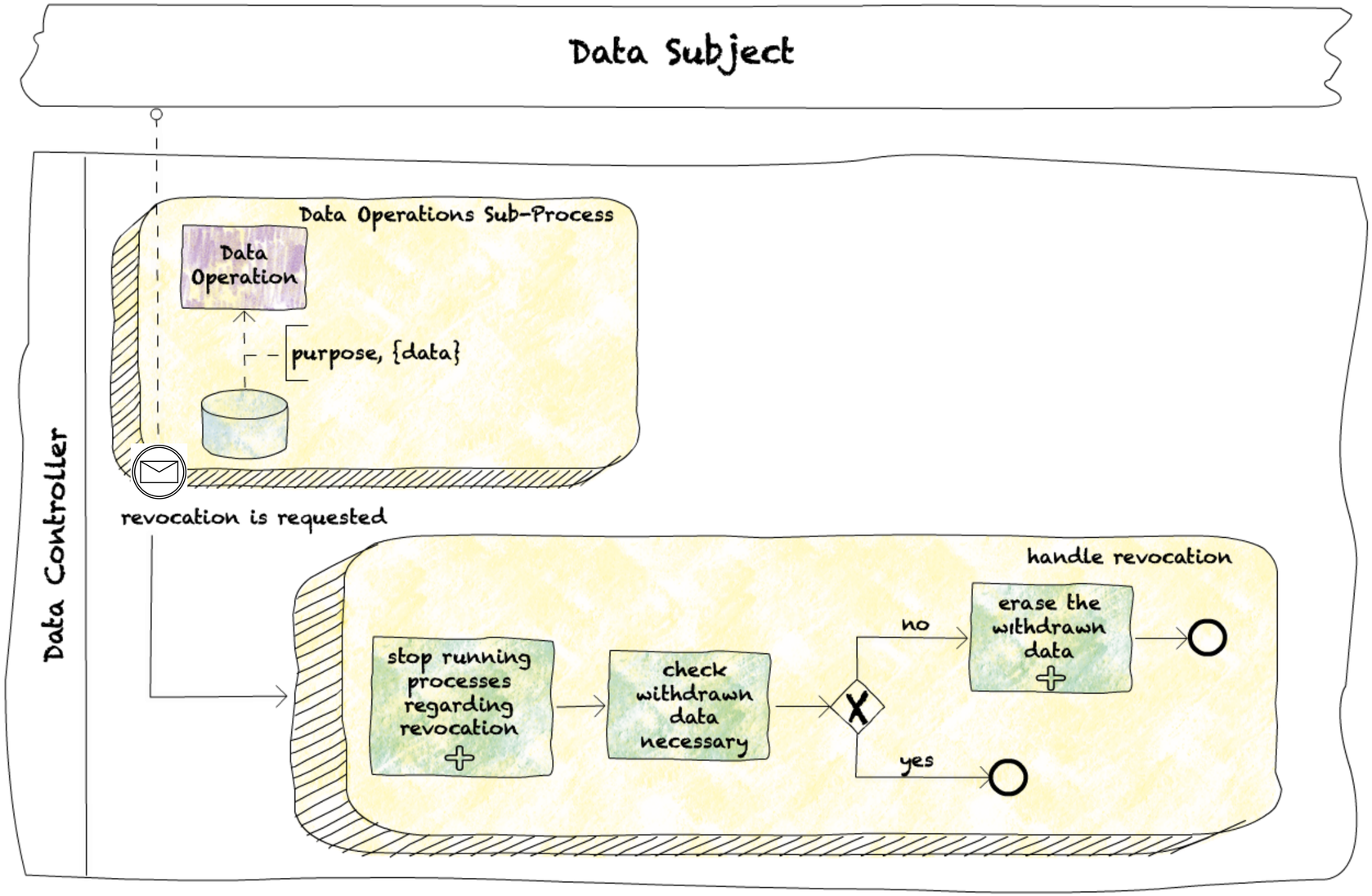
How to handle revocation? → **Revocation Pattern**



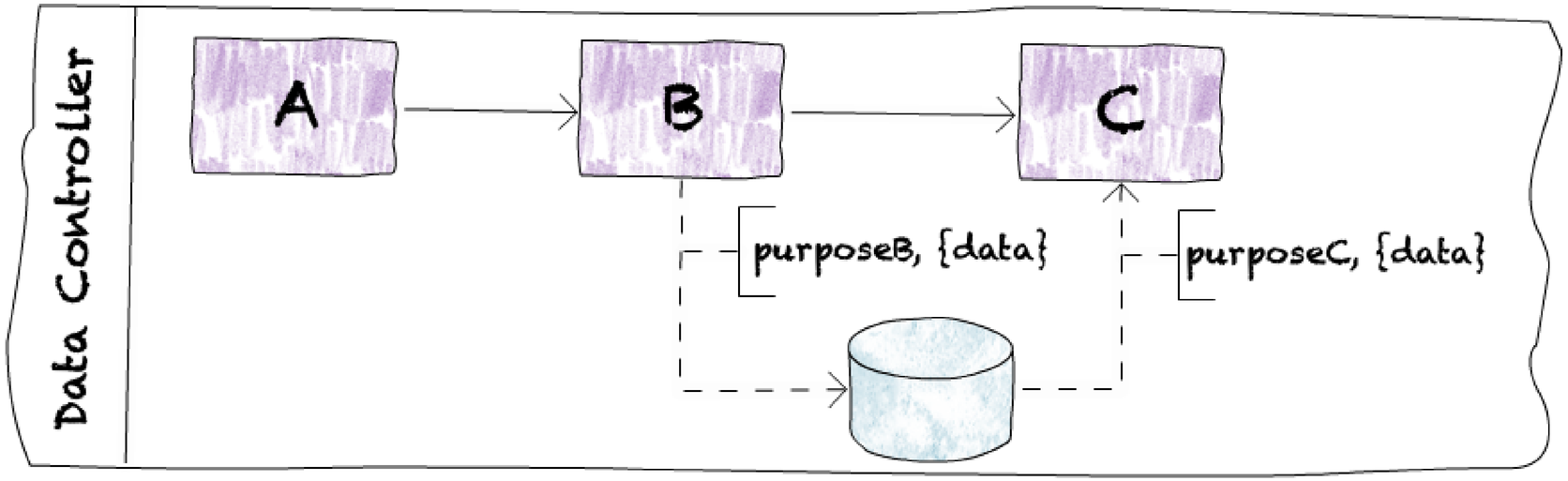
How to handle revocation? → Revocation Pattern



How to handle revocation? → Revocation Pattern

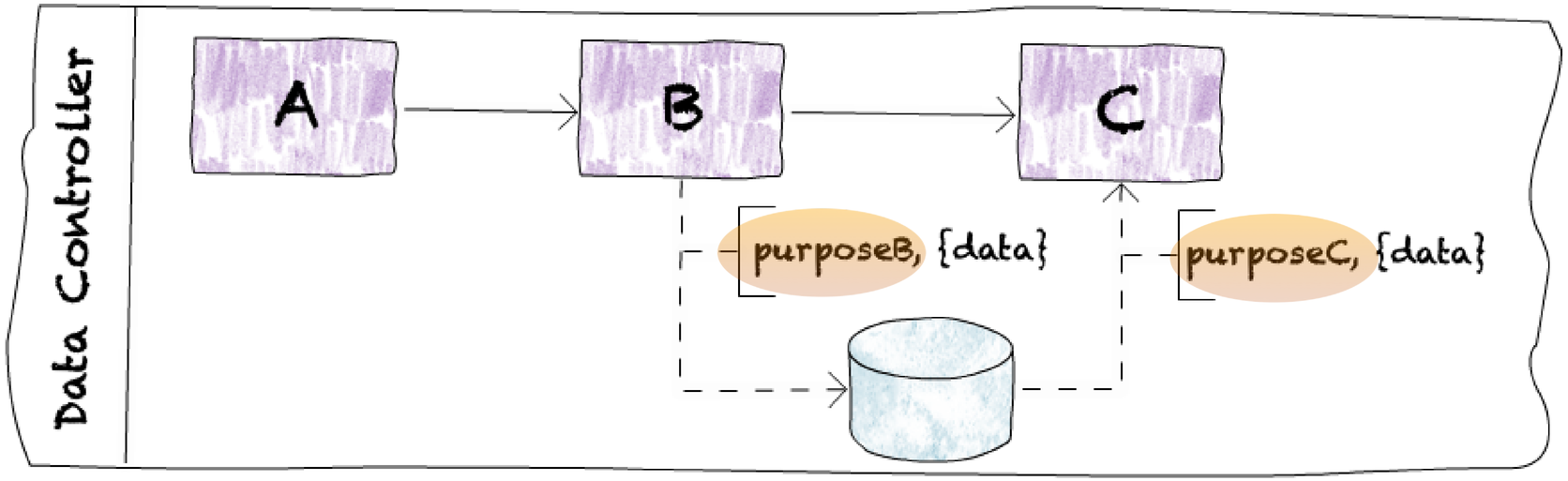


EXAMPLE #1- *AGGREGATED CONSENT*



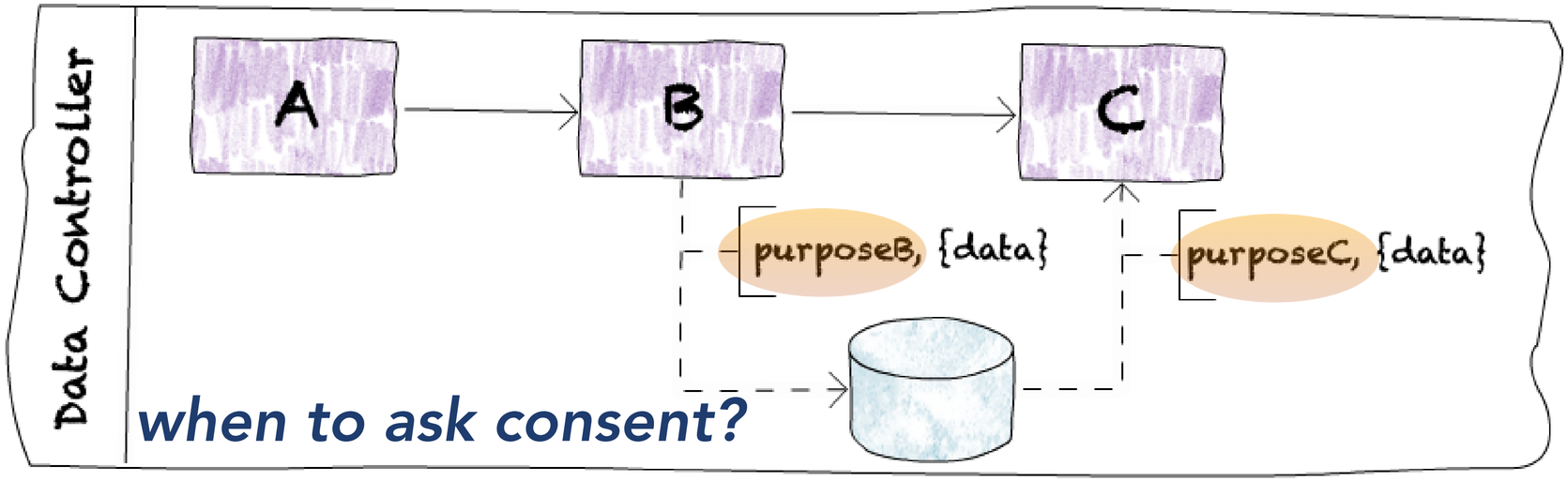
Policy: purposeB & purposeC require consent

EXAMPLE #1- *AGGREGATED CONSENT*



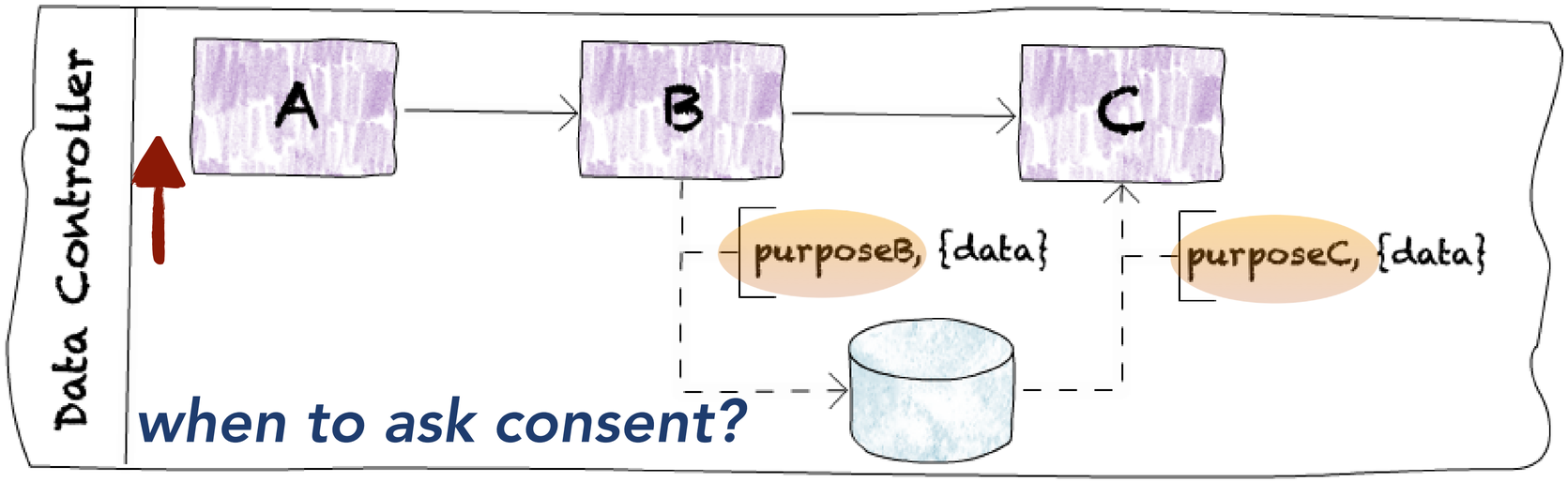
Policy: purposeB & purposeC require consent

EXAMPLE #1- *AGGREGATED CONSENT*



Policy: purposeB & purposeC require consent

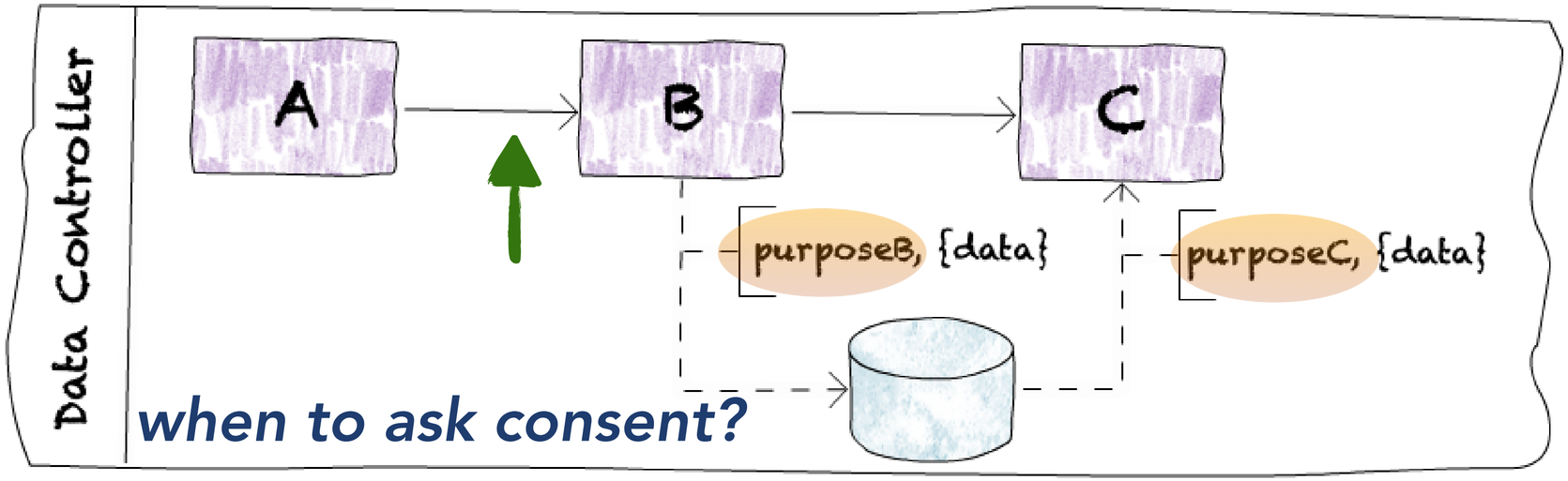
EXAMPLE #1- *AGGREGATED CONSENT*



"Potential" Issue: Consent is obtained yet never used

Policy: purposeB & purposeC require consent

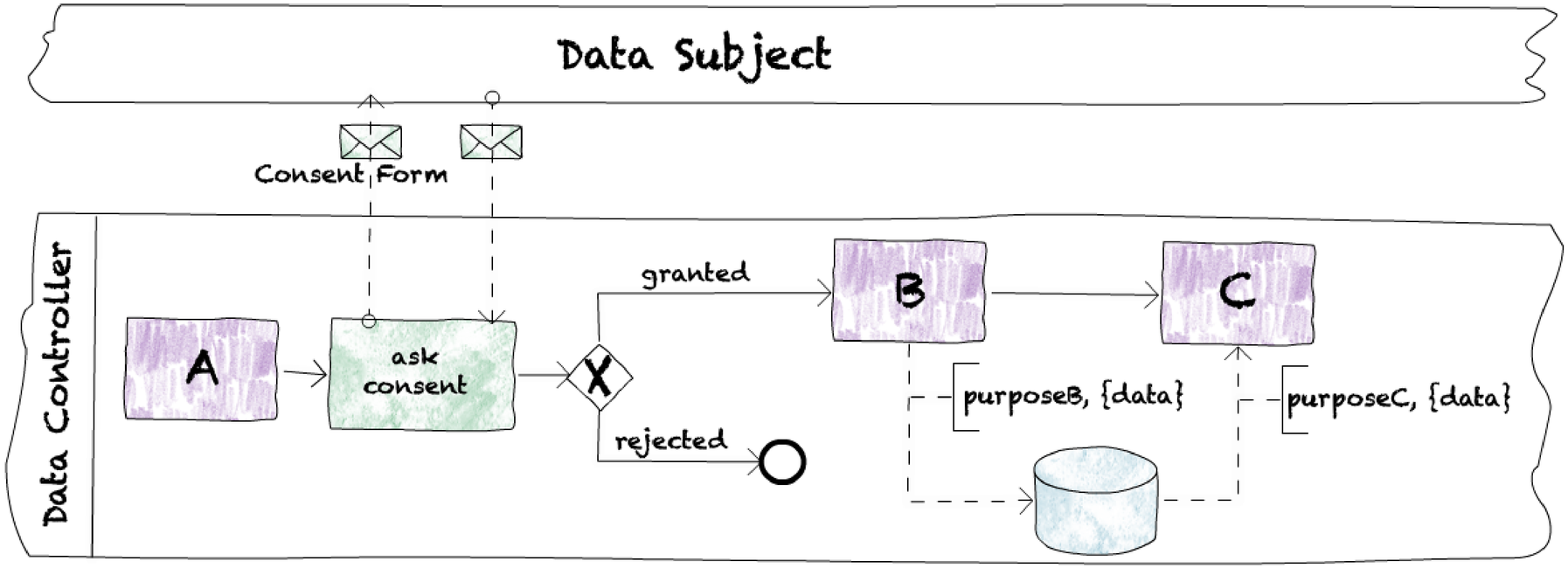
EXAMPLE #1- *AGGREGATED CONSENT*



Strategy: ask it just before data operation to minimize this risk

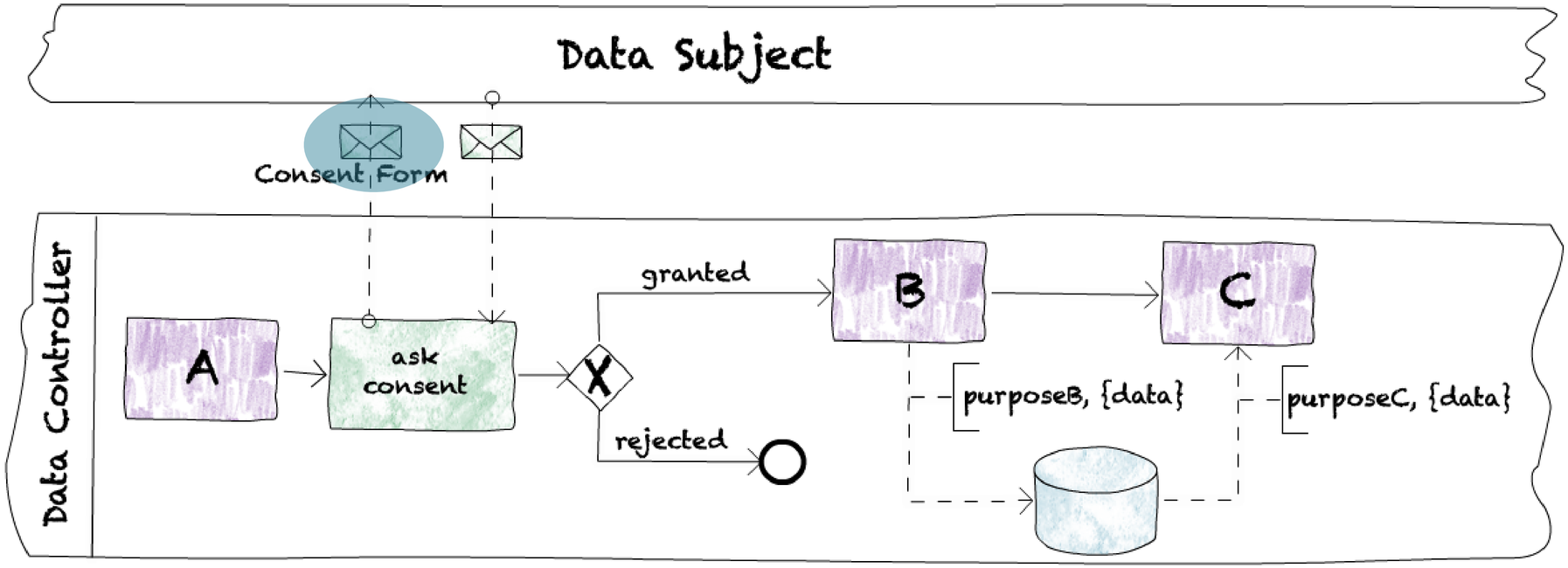
Policy: purposeB & purposeC require consent

EXAMPLE #1- *AGGREGATED CONSENT*



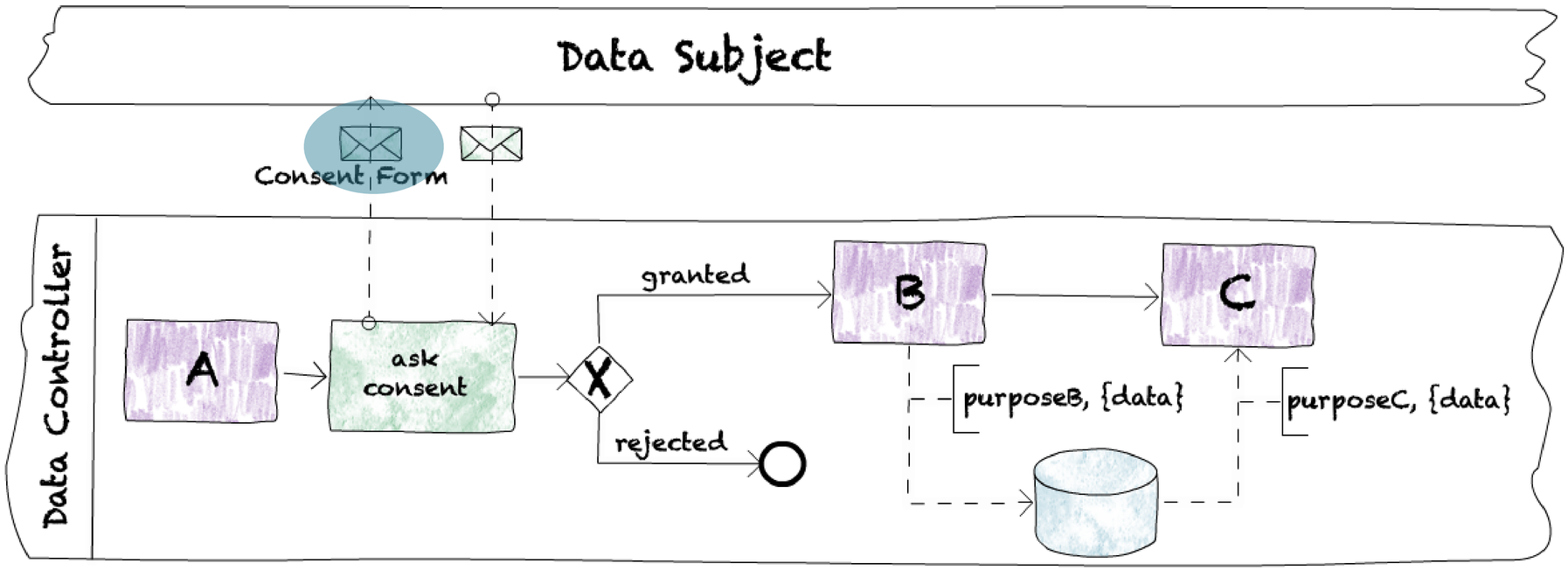
Policy: purposeB & purposeC require consent

EXAMPLE #1- *AGGREGATED CONSENT*



Policy: purposeB & purposeC require consent

EXAMPLE #1- *AGGREGATED CONSENT*



Consent Form

Data Controller

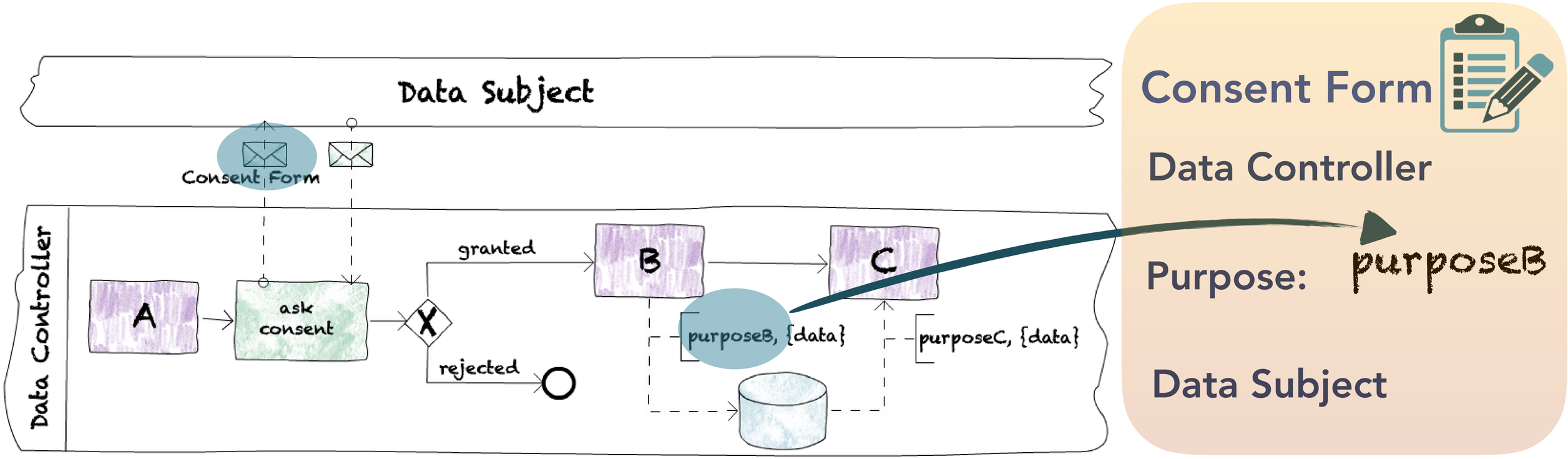
Purpose:

Data Subject

Aggregated Consent Form

Policy: purposeB & purposeC require consent

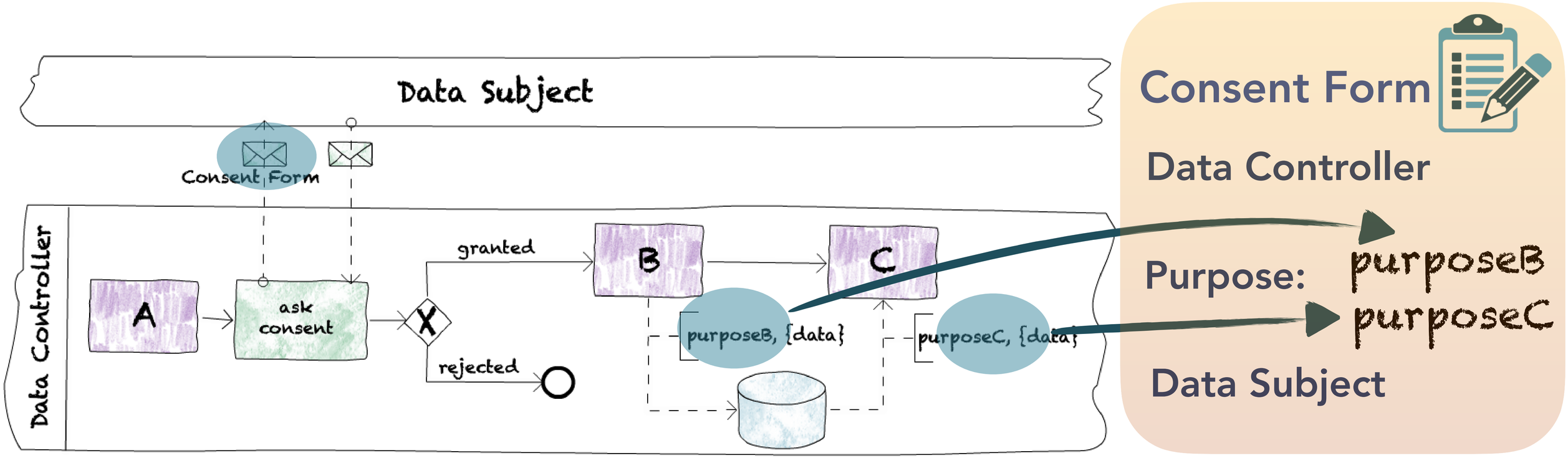
EXAMPLE #1- *AGGREGATED CONSENT*



Aggregated Consent Form

Policy: purposeB & purposeC require consent

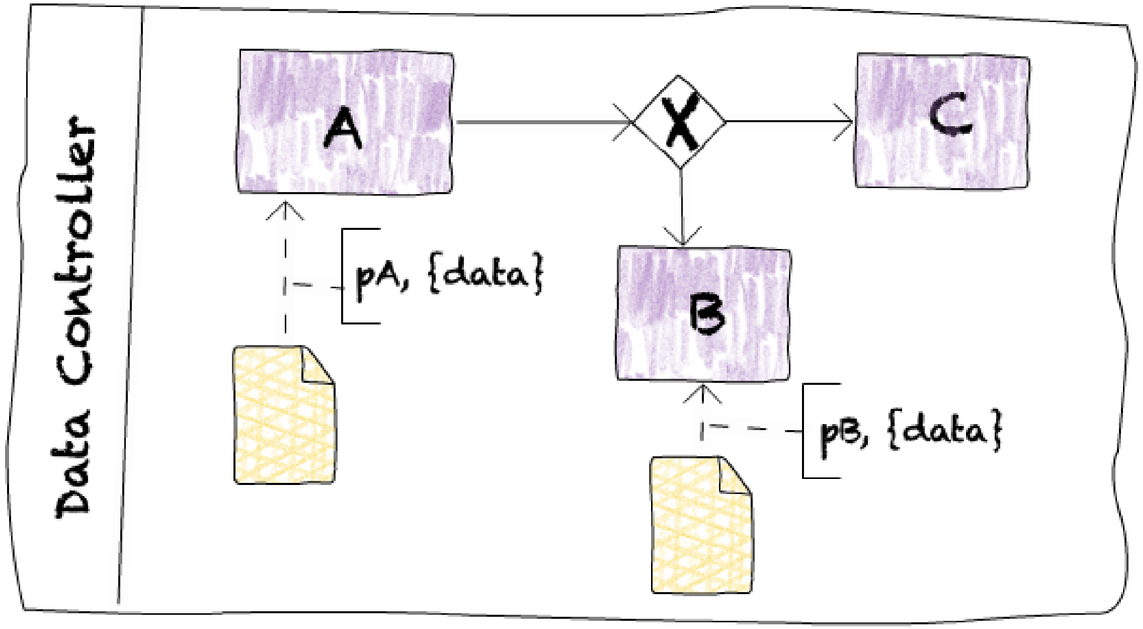
EXAMPLE #1- *AGGREGATED CONSENT*



Aggregated Consent Form

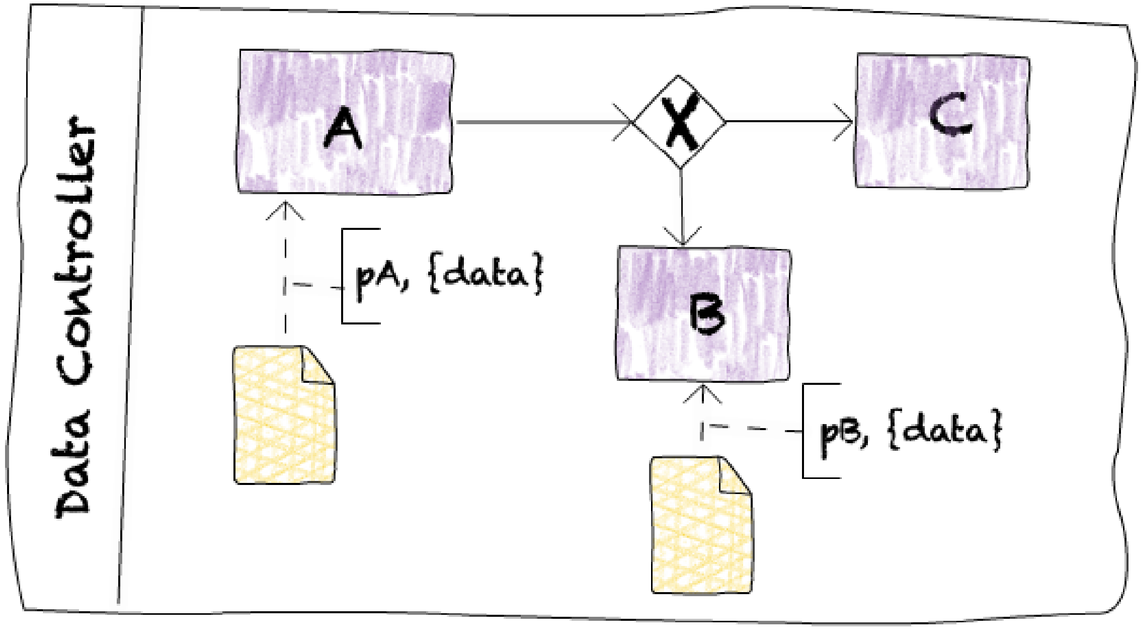
Policy: purposeB & purposeC require consent

EXAMPLE #2 - *SEPARATE CONSENT*



Policy: pA & pB require consent

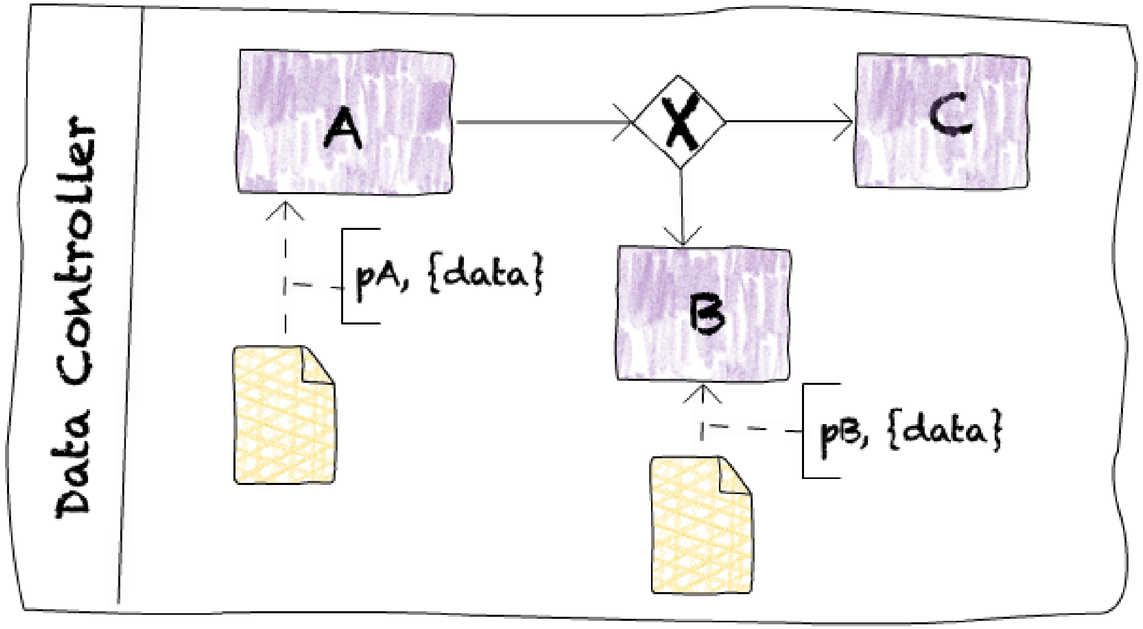
EXAMPLE #2 - *SEPARATE CONSENT*



Aggregated vs Separate Consent Form?

Policy: pA & pB require consent

EXAMPLE #2 - *SEPARATE CONSENT*

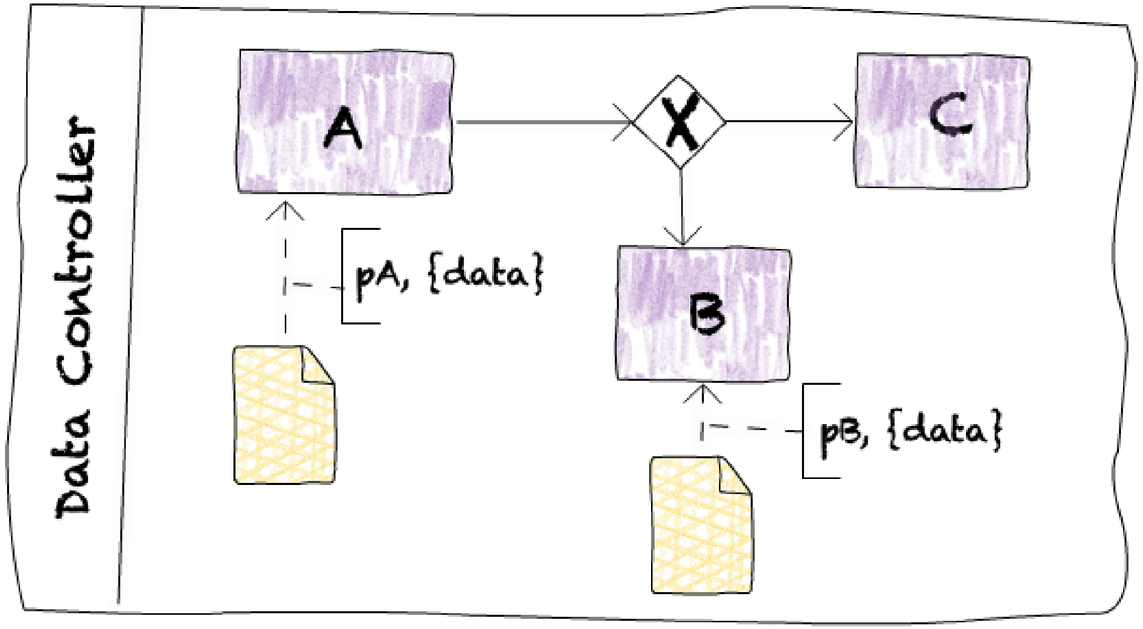


Aggregated vs Separate Consent Form?

"Potential" Issue: Consent is obtained yet never used

Policy: pA & pB require consent

EXAMPLE #2 - *SEPARATE CONSENT*

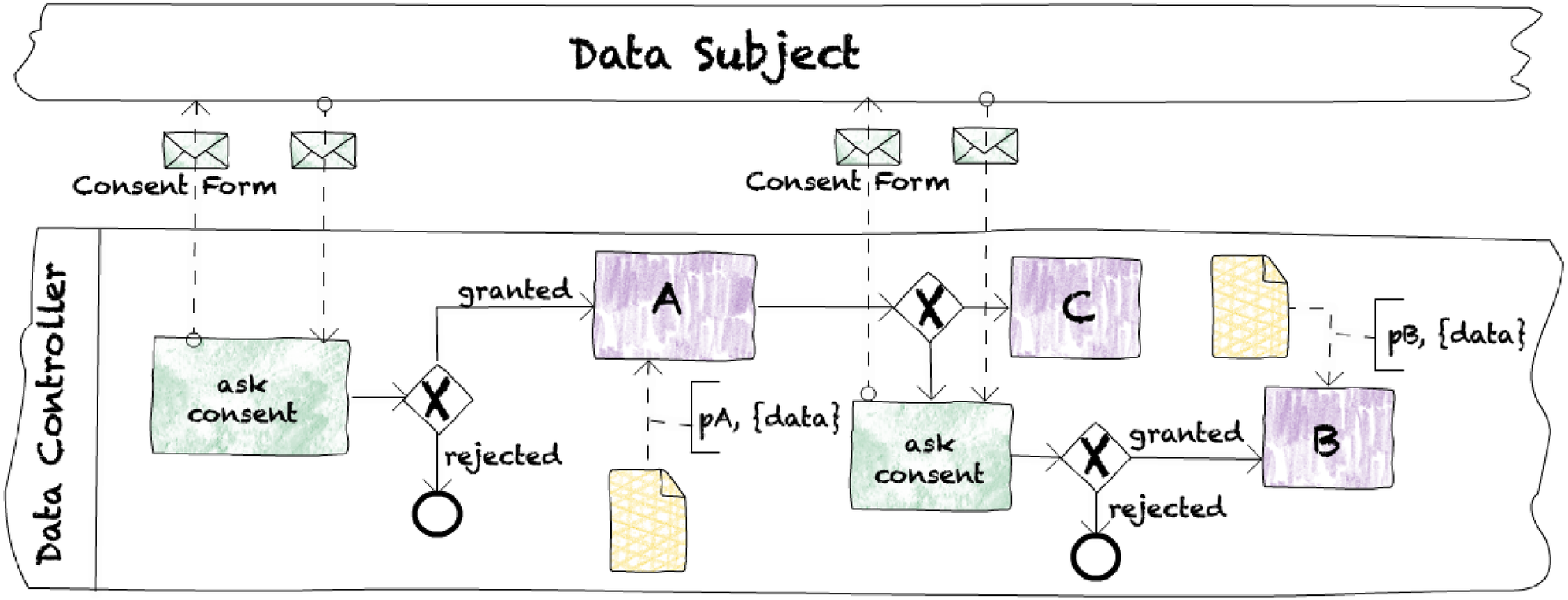


Aggregated vs Separate Consent Form?

"Potential" Issue: Consent is obtained yet never used

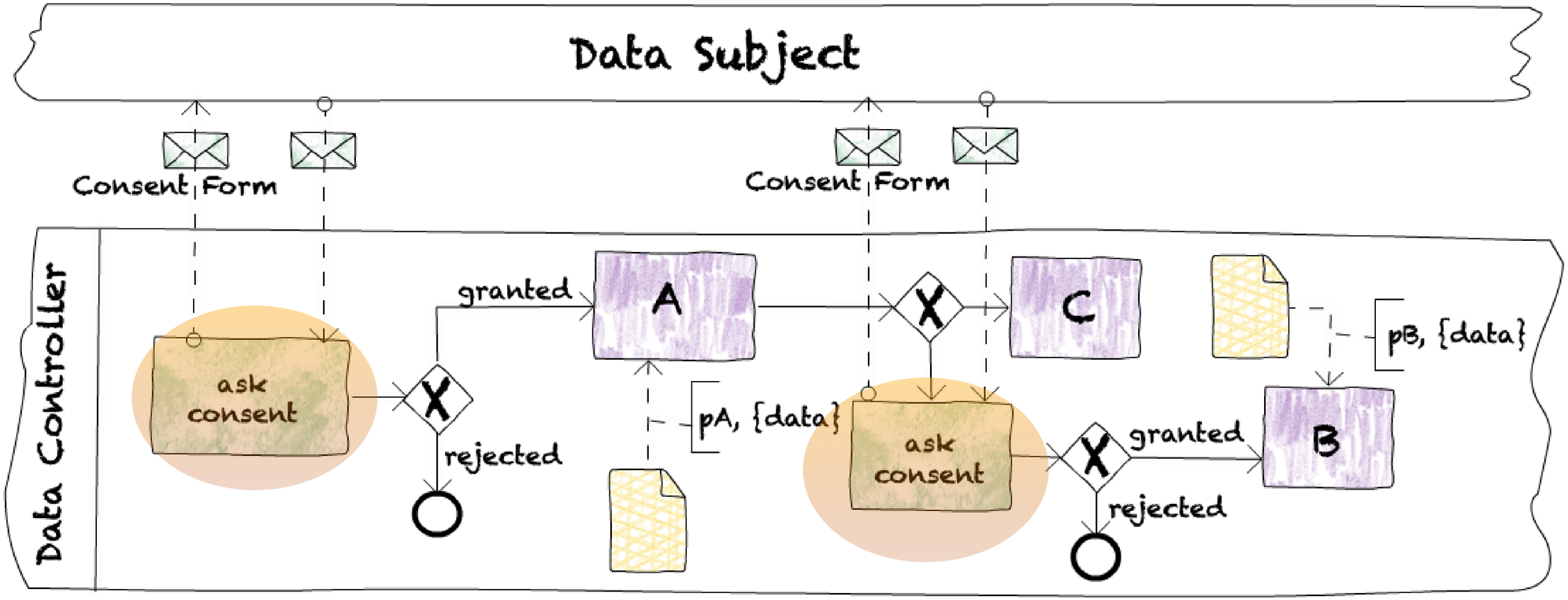
Policy: pA & pB require consent

EXAMPLE #2 - *SEPARATE CONSENT*



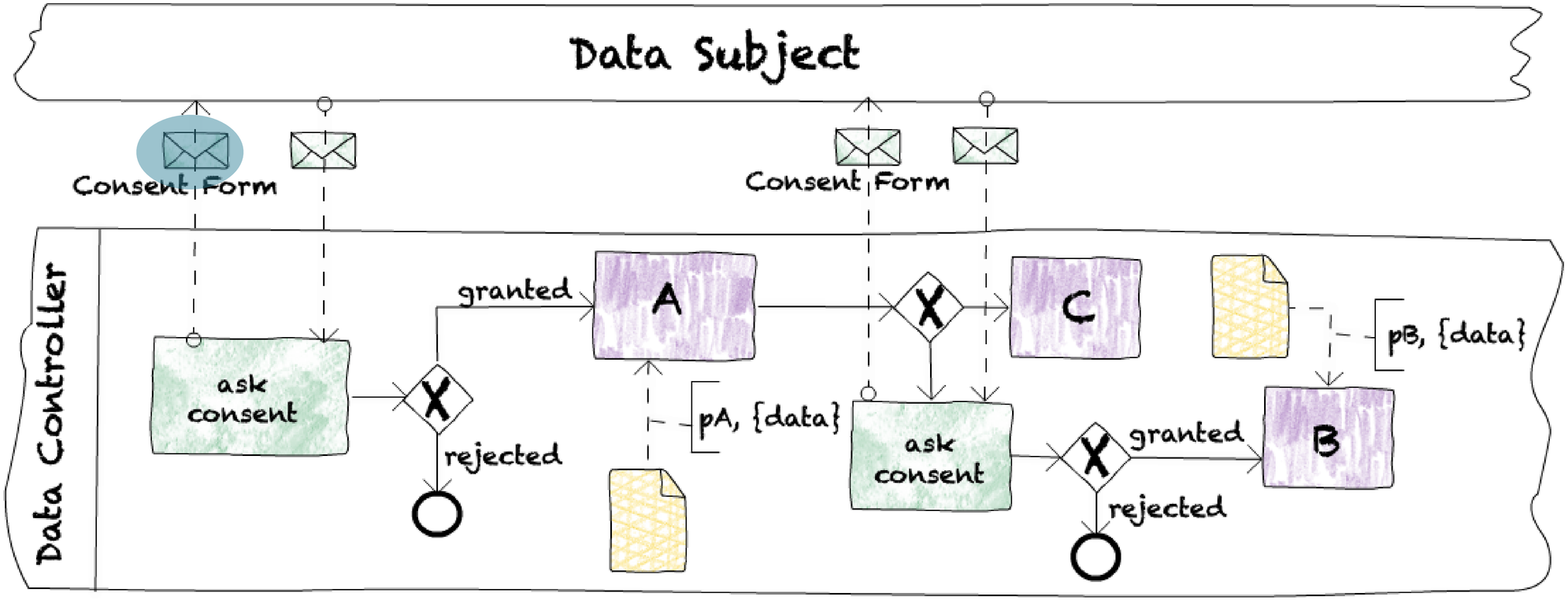
Policy: pA & pB require consent

EXAMPLE #2 - *SEPARATE CONSENT*



Policy: pA & pB require consent

EXAMPLE #2 - *SEPARATE CONSENT*

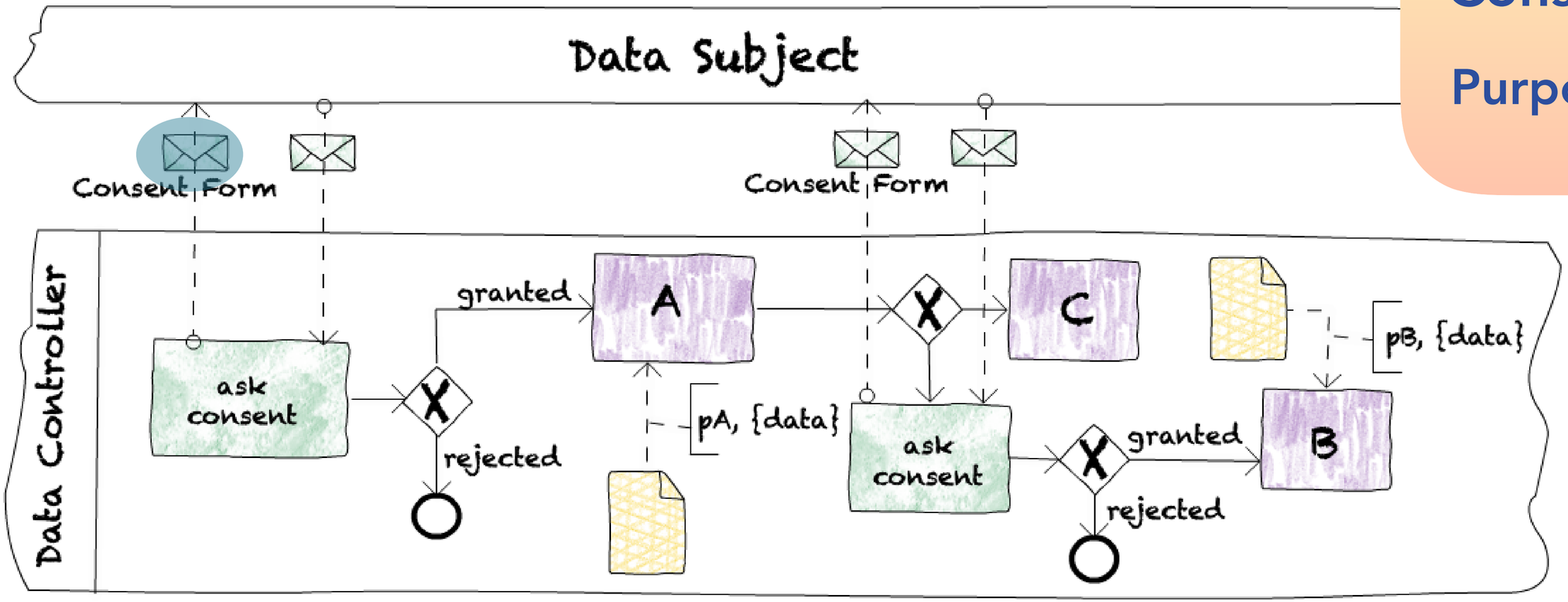


Policy: pA & pB require consent

EXAMPLE #2 - *SEPARATE CONS*

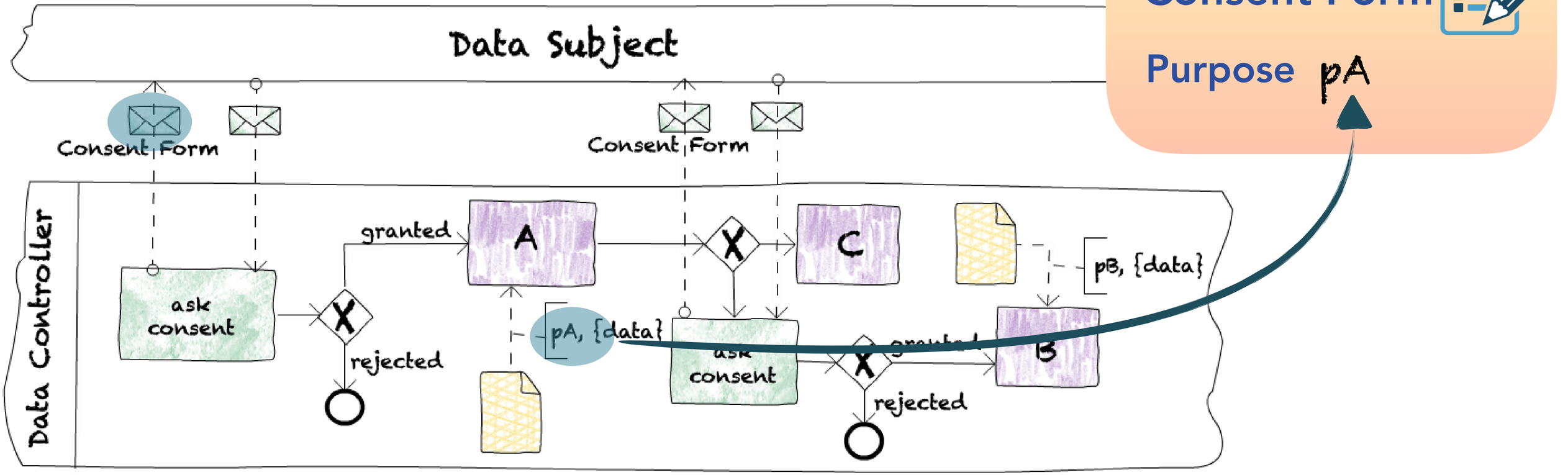
Consent Form

Purpose



Policy: pA & pB require consent

EXAMPLE #2 - *SEPARATE CONS*

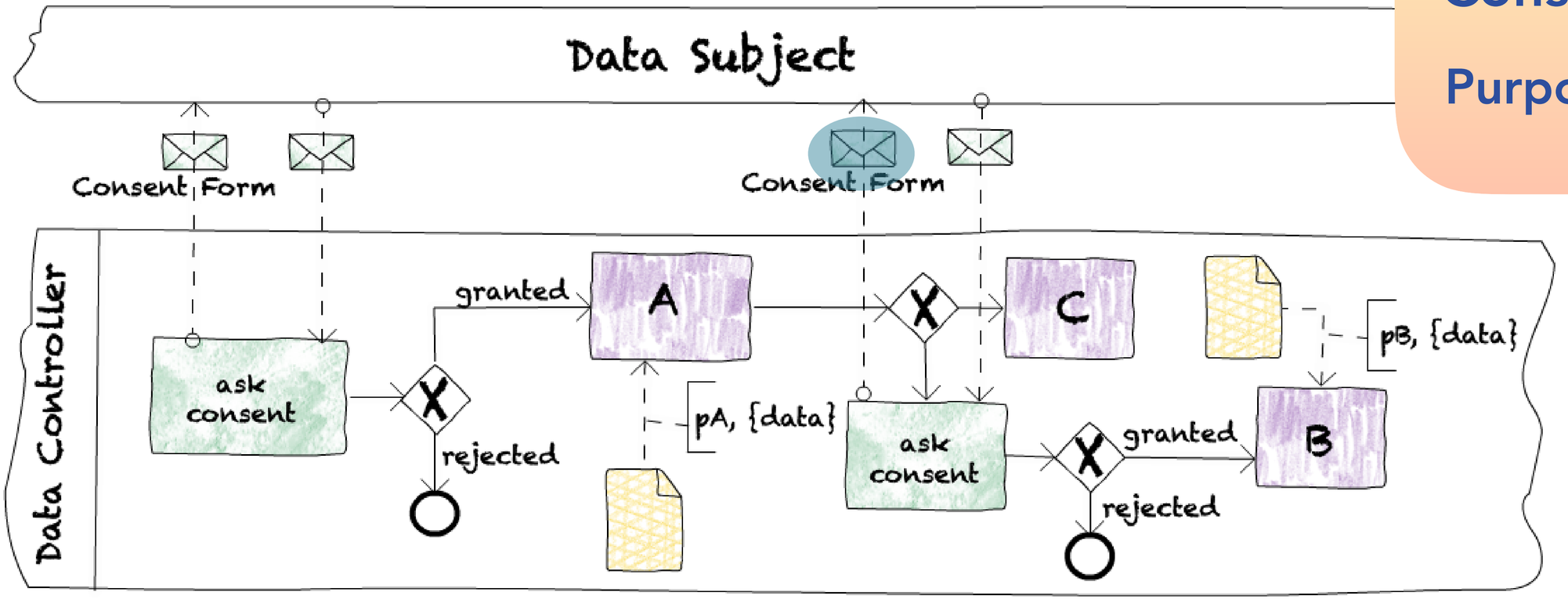


Policy: pA & pB require consent

EXAMPLE #2 - *SEPARATE CONS*

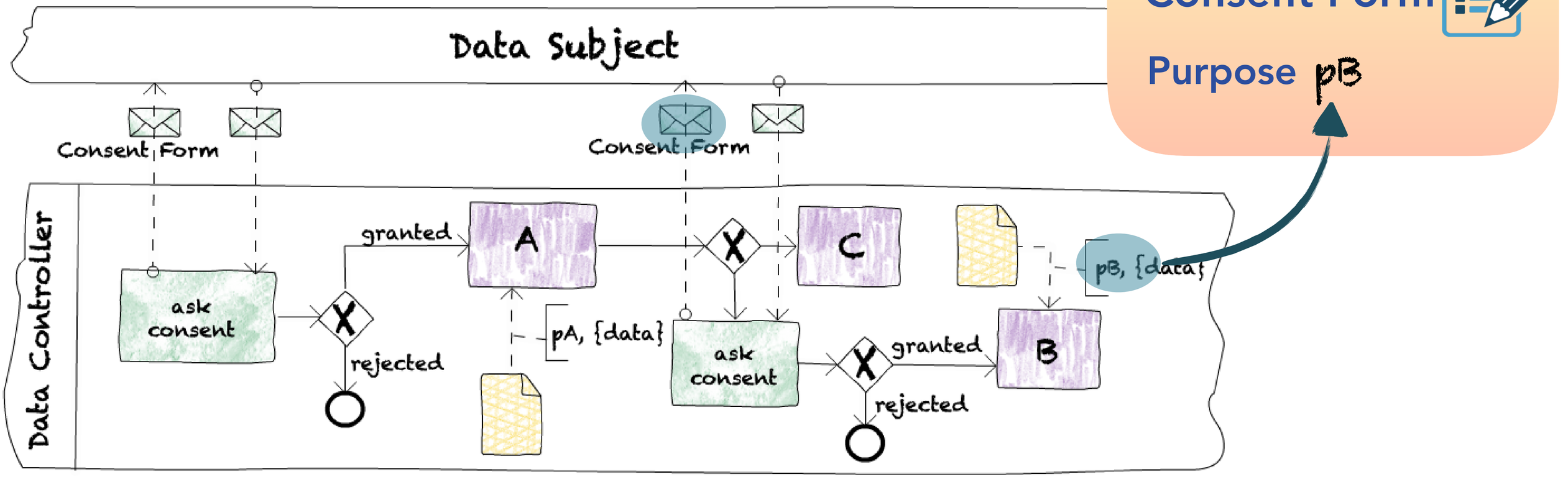
Consent Form

Purpose



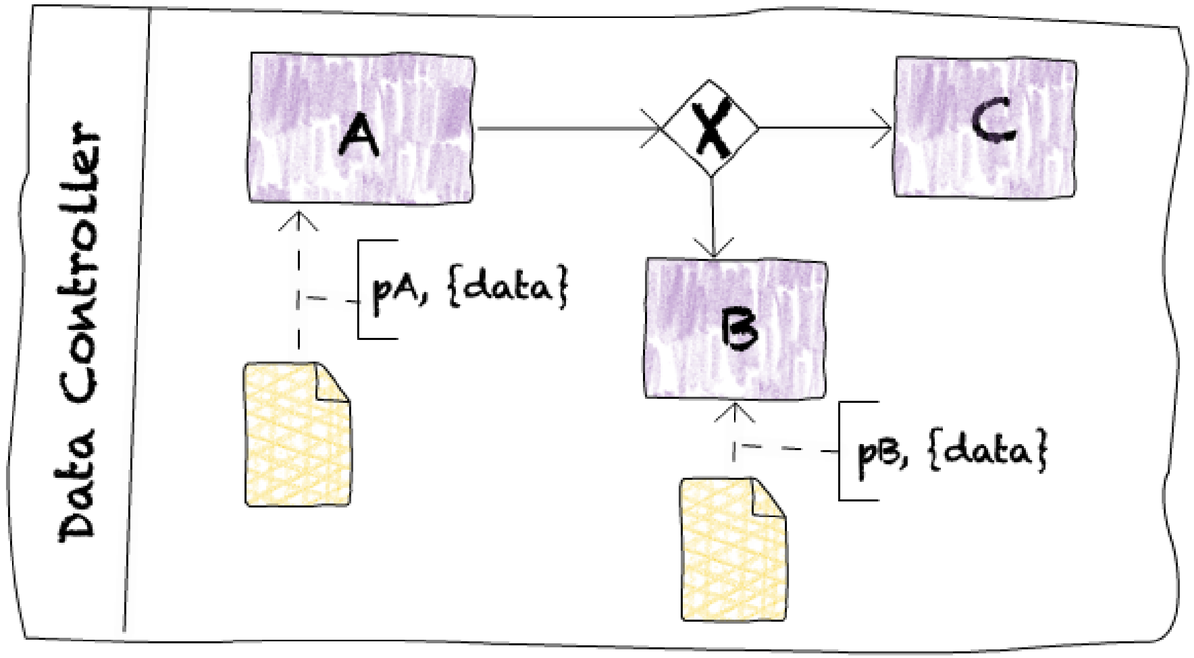
Policy: pA & pB require consent

EXAMPLE #2 - *SEPARATE CONS*



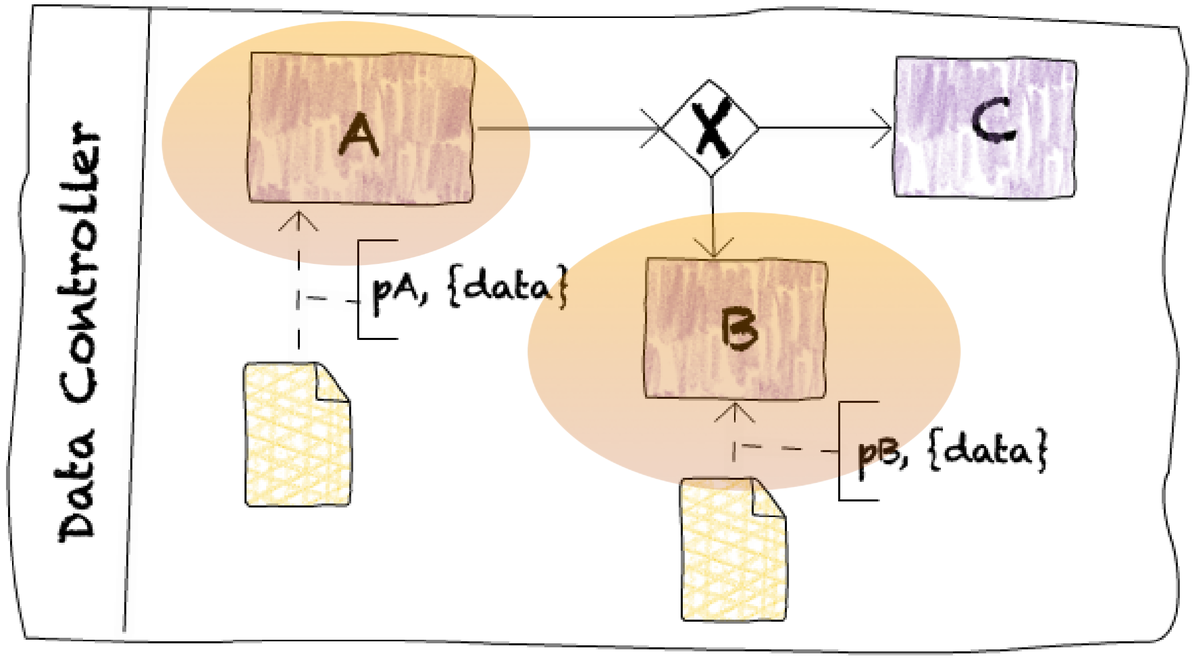
Policy: pA & pB require consent

EXAMPLE #3 - *REVOCATION*



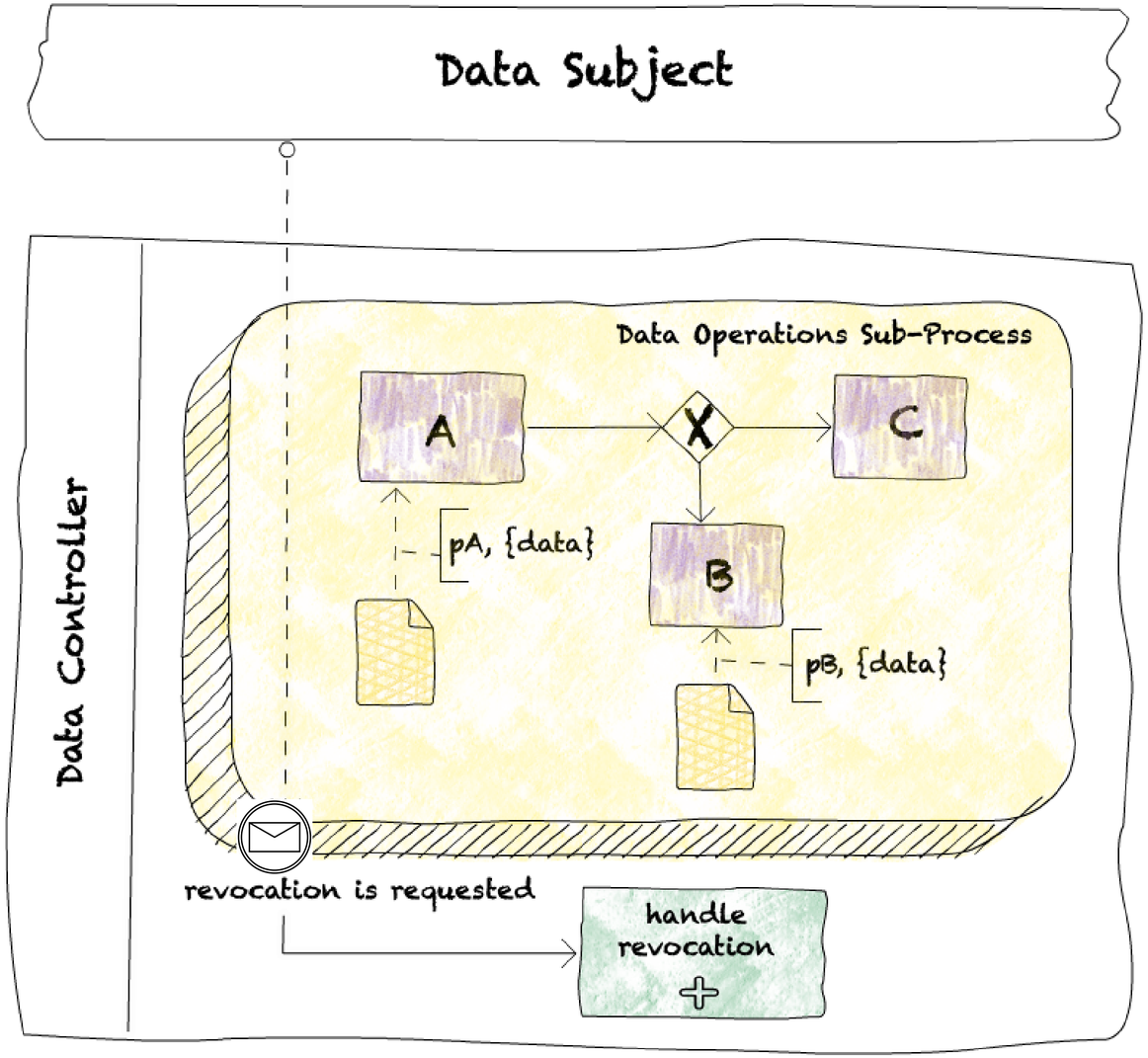
Policy: pA & pB require consent

EXAMPLE #3 - *REVOCATION*

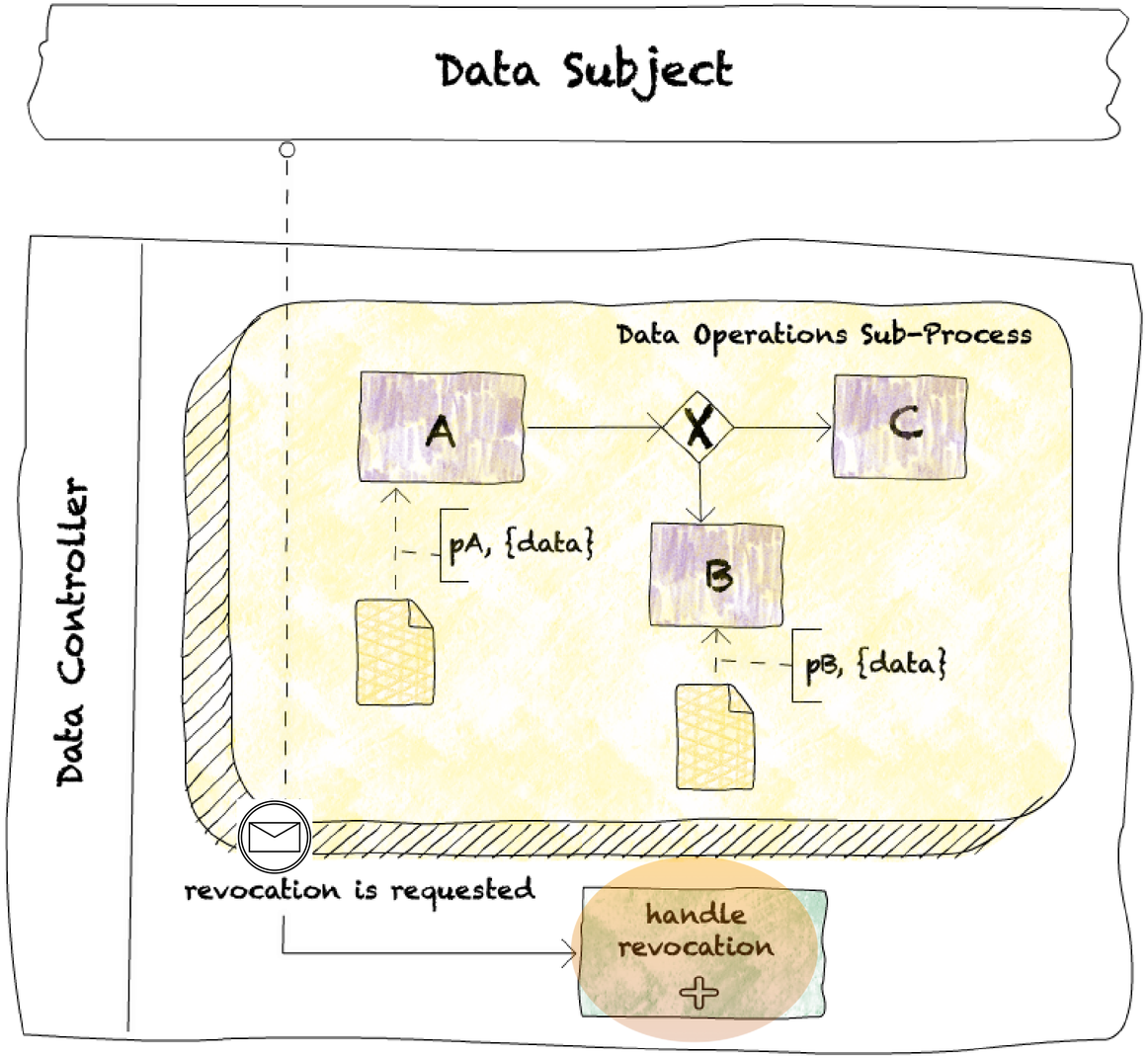


Policy: pA & pB require consent

EXAMPLE #3 - *REVOCATION*

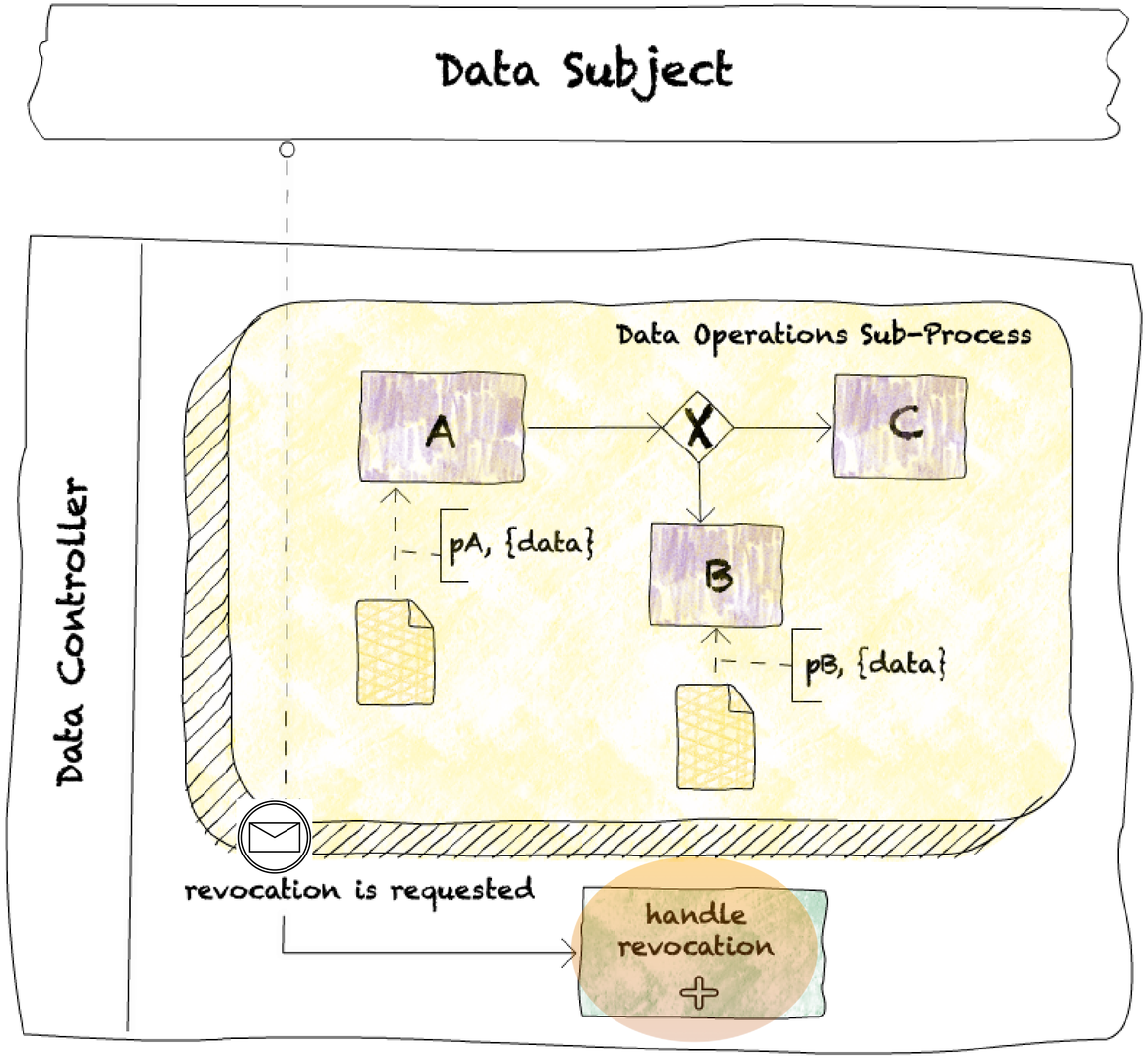


EXAMPLE #3 - *REVOCATION*



Collapsed Sub-Process

EXAMPLE #3 - *REVOCATION*



Collapsed Sub-Process

increases readability

SUMMARY

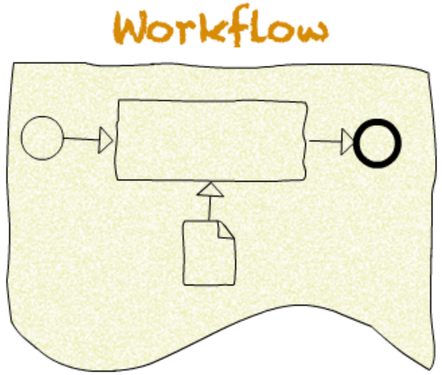
- Organizations processing personal data must consider **consent** & **revocation**

SUMMARY

- Organizations processing personal data must consider **consent** & **revocation**
- **Privacy-by-design** via workflows

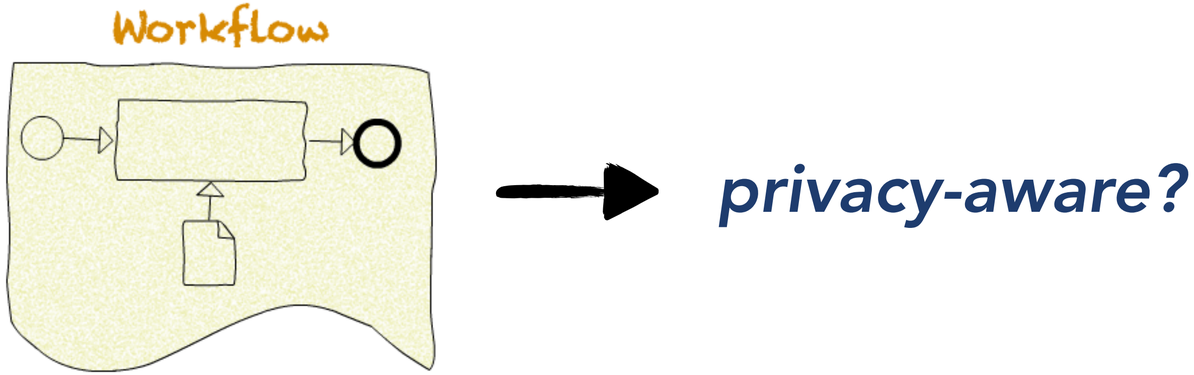
SUMMARY

- Organizations processing personal data must consider **consent** & **revocation**
- **Privacy-by-design** via workflows



SUMMARY

- Organizations processing personal data must consider **consent** & **revocation**
- **Privacy-by-design** via workflows



SUMMARY

- Organizations processing personal data must consider **consent** & **revocation**
- **Privacy-by-design** via workflows

SUMMARY

- Organizations processing personal data must consider **consent** & **revocation**
- **Privacy-by-design** via workflows

- ***What are needed to handle consent in workflows?***

SUMMARY

- Organizations processing personal data must consider **consent** & **revocation**
- **Privacy-by-design** via workflows

- ***What are needed to handle consent in workflows?***
  - **Data-Aware Workflow**

SUMMARY

- Organizations processing personal data must consider **consent** & **revocation**
- **Privacy-by-design** via workflows

- ***What are needed to handle consent in workflows?***
  - **Data-Aware Workflow**  **Consent Policy** 

SUMMARY

- Organizations processing personal data must consider **consent** & **revocation**
- **Privacy-by-design** via workflows

- ***What are needed to handle consent in workflows?***
  - **Data-Aware Workflow**  **Consent Policy**  **Consent Form** 

- ***Approach: Design Patterns***

- *Approach: Design Patterns*
  - **Consent Pattern**

- *Approach: Design Patterns*
  - **Consent Pattern**
  - **Revocation Pattern**

- *Approach: Design Patterns*
  - **Consent Pattern**
  - **Revocation Pattern**

OUTLOOK

- Analysis of the **optimality** of the design patterns

- *Approach: Design Patterns*
  - **Consent Pattern**
  - **Revocation Pattern**

OUTLOOK

- Analysis of the **optimality** of the design patterns
- Automatic transformation

- *Approach: Design Patterns*
  - **Consent Pattern**
  - **Revocation Pattern**

Thank you!!!

OUTLO

- Analysis of the **optimality** of the design patterns
- Automatic transformation

- *Approach: Design Patterns*
  - **Consent Pattern**
  - **Revocation Pattern**

OUTLOOK

- Analysis of the **optimality** of the design patterns
- Automatic transformation