DPOE

Data Privacy Observation Engine

Jake Tom (jaketom@ut.ee)
Raimundas Matulevičius, Peeter Laud
University of Tartu, 15.11.18

DPOE

(pronounced dee-po)

Web application **for DPOs**

Provides overview of **privacy management status** of organization (wrt. GDPR)

Input: Business process models (in BPMN)

Output: Compliance report and visualization

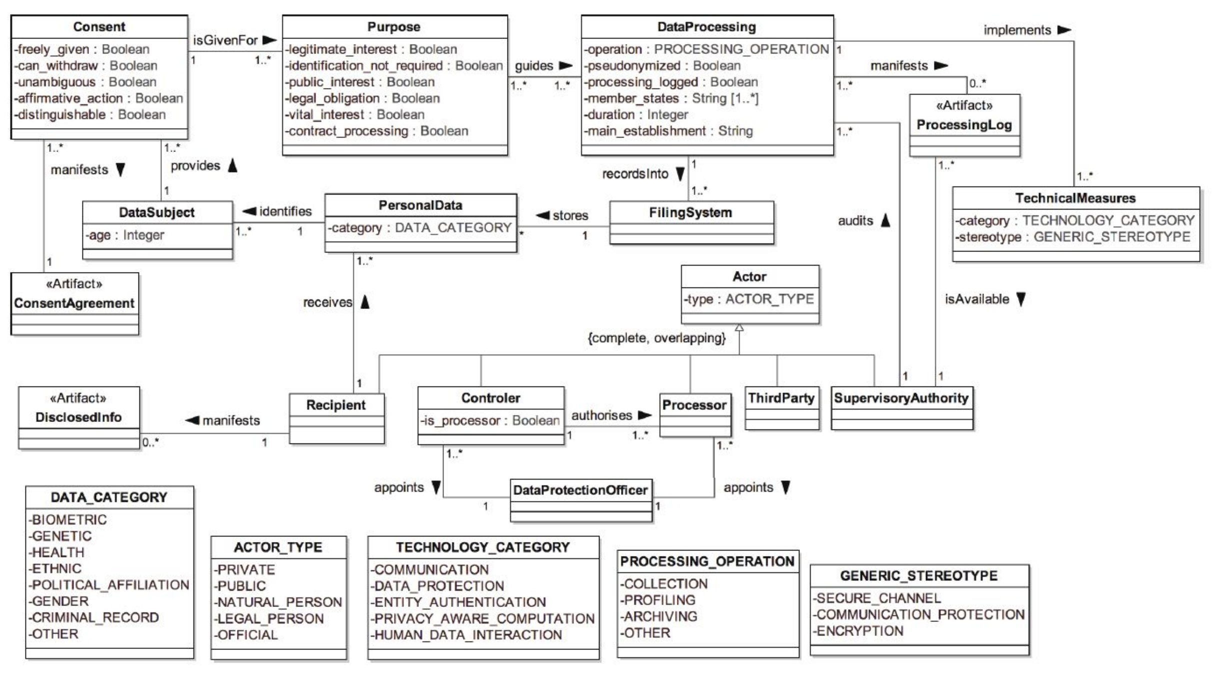
Conceptual foundation [1]

Main **entities**

Important **concepts**

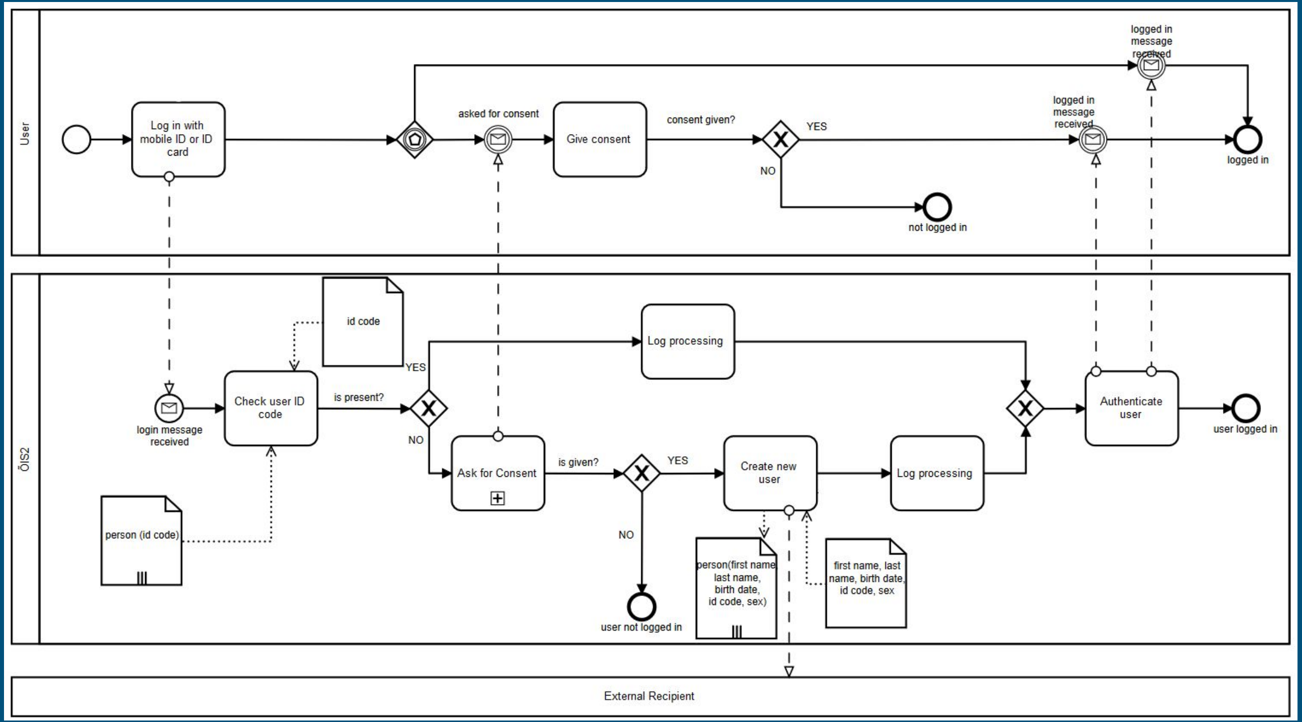
Relationships (What + how)

Data subject **rights**



Screenshots from demo (Slides 6-9)

Input


User
Log in with mobile ID or ID card
asked for consent
Give consent
consent given?
YES
NO
not logged in
logged in message received
logged in message received
logged in
ÕIS2
id code
login message received
Check user ID code
is present?
YES
NO
Log processing
Ask for Consent
is given?
YES
NO
user not logged in
Create new user
Log processing
Authenticate user
user logged in
person (id code)
person(first name last name, birth date, id code, sex)
first name, last name, birth date, id code, sex
External Recipient

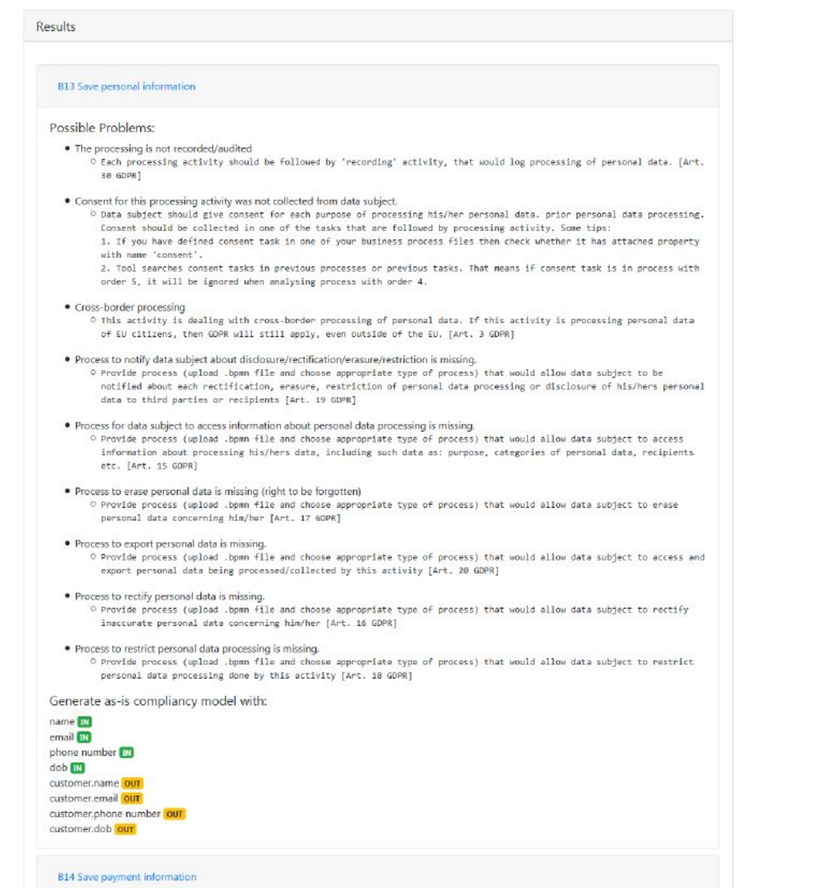
Output (text)

Output is provided as **text** (list of potential violations) or **visualization** (instantiated view of conceptual model)

Visualizations can be generated from the perspective of **individual data attributes**

Maps the BPMN model onto the conceptual model and **identifies missing attributes, links, etc.**

Traces the missing links to the articles they came from in the GDPR



Results

B13 Save personal information

Possible Problems:

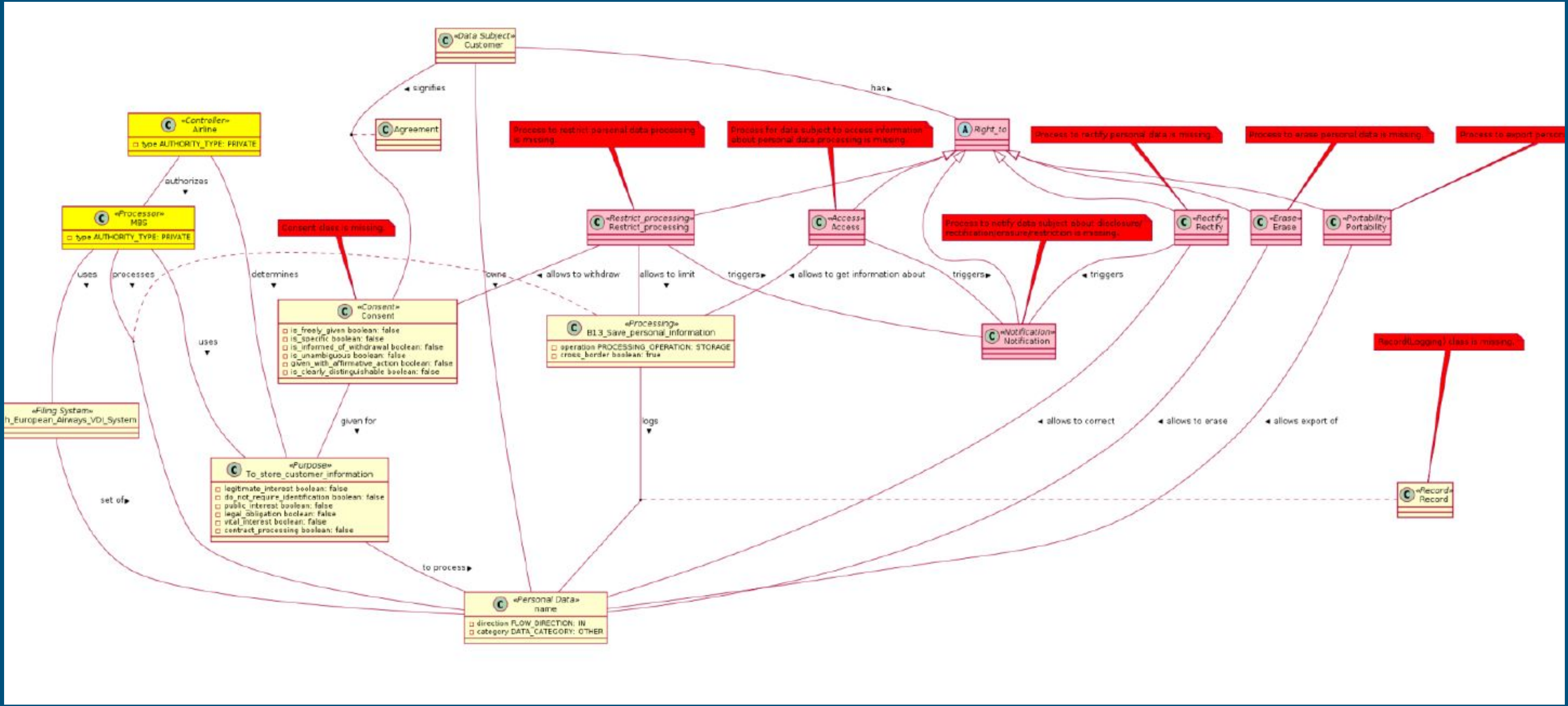
- The processing is not recorded/audited
    - Each processing activity should be followed by 'recording' activity, that would log processing of personal data. [Art. 30 GDPR]
- Consent for this processing activity was not collected from data subject.
    - Data subject should give consent for each purpose of processing his/her personal data. prior personal data processing. Consent should be collected in one of the tasks that are followed by processing activity. Some tips:
      1. If you have defined consent task in one of your business process files then check whether it has attached property with name 'consent'.
      2. Tool searches consent tasks in previous processes or previous tasks. That means if consent task is in process with order 5, it will be ignored when analysing process with order 4.
- Cross-border processing
    - This activity is dealing with cross-border processing of personal data. If this activity is processing personal data of EU citizens, then GDPR will still apply, even outside of the EU. [Art. 3 GDPR]
- Process to notify data subject about disclosure/rectification/erasure/restriction is missing.
    - Provide process (upload .bpmn file and choose appropriate type of process) that would allow data subject to be notified about each rectification, erasure, restriction of personal data processing or disclosure of his/hers personal data to third parties or recipients [Art. 19 GDPR]
- Process for data subject to access information about personal data processing is missing.
    - Provide process (upload .bpmn file and choose appropriate type of process) that would allow data subject to access information about processing his/hers data, including such data as: purpose, categories of personal data, recipients etc. [Art. 15 GDPR]
- Process to erase personal data is missing (right to be forgotten)
    - Provide process (upload .bpmn file and choose appropriate type of process) that would allow data subject to erase personal data concerning him/her [Art. 17 GDPR]
- Process to export personal data is missing.
    - Provide process (upload .bpmn file and choose appropriate type of process) that would allow data subject to access and export personal data being processed/collected by this activity [Art. 20 GDPR]
- Process to rectify personal data is missing.
    - Provide process (upload .bpmn file and choose appropriate type of process) that would allow data subject to rectify inaccurate personal data concerning him/her [Art. 16 GDPR]
- Process to restrict personal data processing is missing.
    - Provide process (upload .bpmn file and choose appropriate type of process) that would allow data subject to restrict personal data processing done by this activity [Art. 18 GDPR]

Generate as-is compliancy model with:

name IN
email IN
phone number IN
dob IN
customer.name OUT
customer.email OUT
customer.phone number OUT
customer.dob OUT

B14 Save payment information

Output (Visualization)


C «Data Subject» Customer
◂ signifies
has ▸
C Agreement
C «Controller» Airline
□ type AUTHORITY_TYPE: PRIVATE
authorizes ▾
C «Processor» MBS
□ type AUTHORITY_TYPE: PRIVATE
uses ▾
processes ▾
determines ▾
uses ▾
owns ▾
Consent class is missing.
C «Consent» Consent
□ is_freely_given boolean: false
□ is_specific boolean: false
□ is_informed_of_withdrawal boolean: false
□ is_unambiguous boolean: false
□ given_with_affirmative_action boolean: false
□ is_clearly_distinguishable boolean: false
given for ▾
«Filing System» h_European_Airways_VDI_System
set of ▸
C «Purpose» To_store_customer_information
□ legitimate_interest boolean: false
□ do_not_require_identification boolean: false
□ public_interest boolean: false
□ legal_obligation boolean: false
□ vital_interest boolean: false
□ contract_processing boolean: false
to process ▸
C «Personal Data» name
□ direction FLOW_DIRECTION: IN
□ category DATA_CATEGORY: OTHER
Process to restrict personal data processing is missing.
C «Restrict_processing» Restrict_processing
◂ allows to withdraw
allows to limit ▾
triggers ▸
Process for data subject to access information about personal data processing is missing.
C «Access» Access
◂ allows to get information about
triggers ▸
C «Processing» B13_Save_personal_information
□ operation PROCESSING_OPERATION: STORAGE
□ cross_border boolean: true
logs ▾
A Right_to
Process to notify data subject about disclosure/rectification/erasure/restriction is missing.
◂ triggers
C «Notification» Notification
Process to rectify personal data is missing.
C «Rectify» Rectify
Process to erase personal data is missing.
C «Erase» Erase
Process to export person
C «Portability» Portability
◂ allows to correct
◂ allows to erase
◂ allows export of
Record(Logging) class is missing.
C «Record» Record

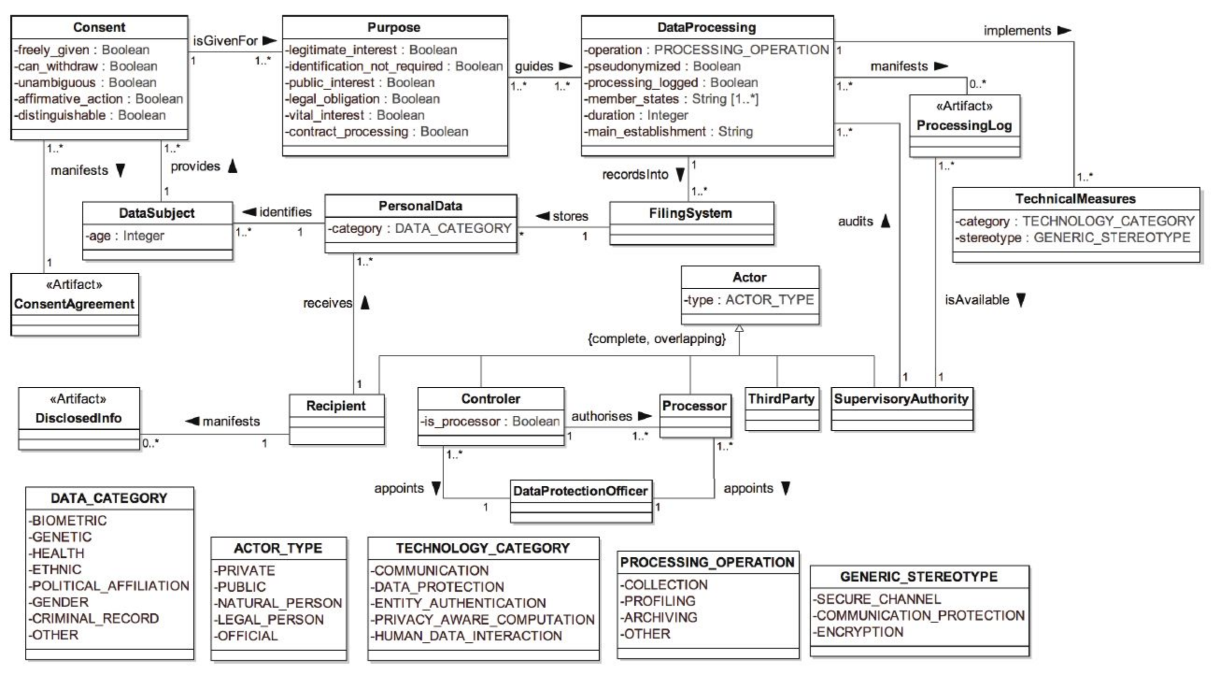
Conceptual foundation [1]

Main **entities**

Important **concepts**

Relationships (What + how)

Data subject **rights**



Goal

Ease the life of a DPO

Reduce manual overhead of DPO tasks

Transparency of data flow

Provide insights into **overlooked compliance aspects**

Currently underway

Legal validation of conceptual model

Our model is **subjective**

Complete representation is **not our goal**

But we do need the **most important aspects**

And we need the information depicted to be **accurate and meaningful**

In the pipeline

Quality of life features for DPOs

Internal privacy goals vs GDPR

Aggregating information from interviews **(conflict identification + communication)**

Cross-project analysis

Privacy-enhanced BPMN [2]

Data lifecycle view (from acquisition to deletion)

In the pipeline

Quality of life features for DPOs

Evidence artifact management

Evidence linking

Full-fledged **report** (ex. Pdf download)

Historic privacy management comparison of reports

Are these goals aligned with what you need as DPOs?

What do you use in your workflow currently?

(ja sinu küsimused)

References

[1] Conceptual Representation of the GDPR: Model and Application Directions, Jake Tom et al. (2018)

[2] PE-BPMN: Privacy-Enhanced Business Process Model and Notation, Pille Pullonen et al. (2017)

Contact

If you’ have questions, feedback or would like to be involved in the enhancement of this work, get in touch!

jaketom@ut.ee
+372 58437042