Istituto di Scienza e Tecnologie dell'Informazione “A. Faedo”
Software Engineering and Dependable Computing Laboratory

Authorization Systems as Privacy Enhancing Technology: An integrated Framework

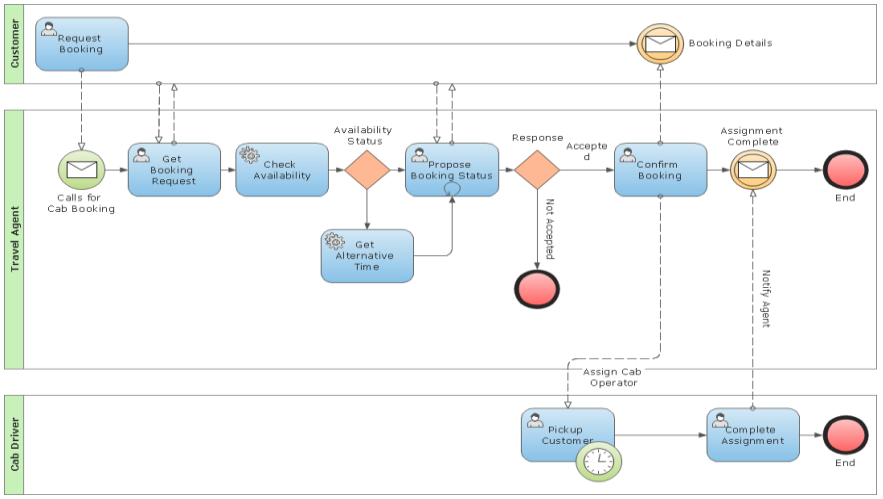
Eda Marchetti

Agenda

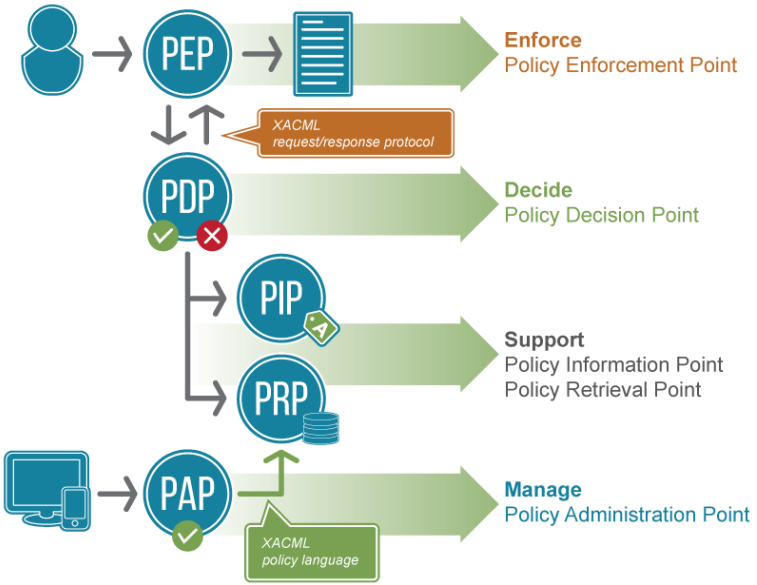
- ✓Business process and Access Control
- ✓ BP-based Access control for GDPR compliance
  - ✓Procedural steps
  - ✓A possible integration
- ✓Conclusions and future directions

Business Process (BP) - Access Control System (AC)

BP is a graphic representation of a process, similar to flowchart, can be executable



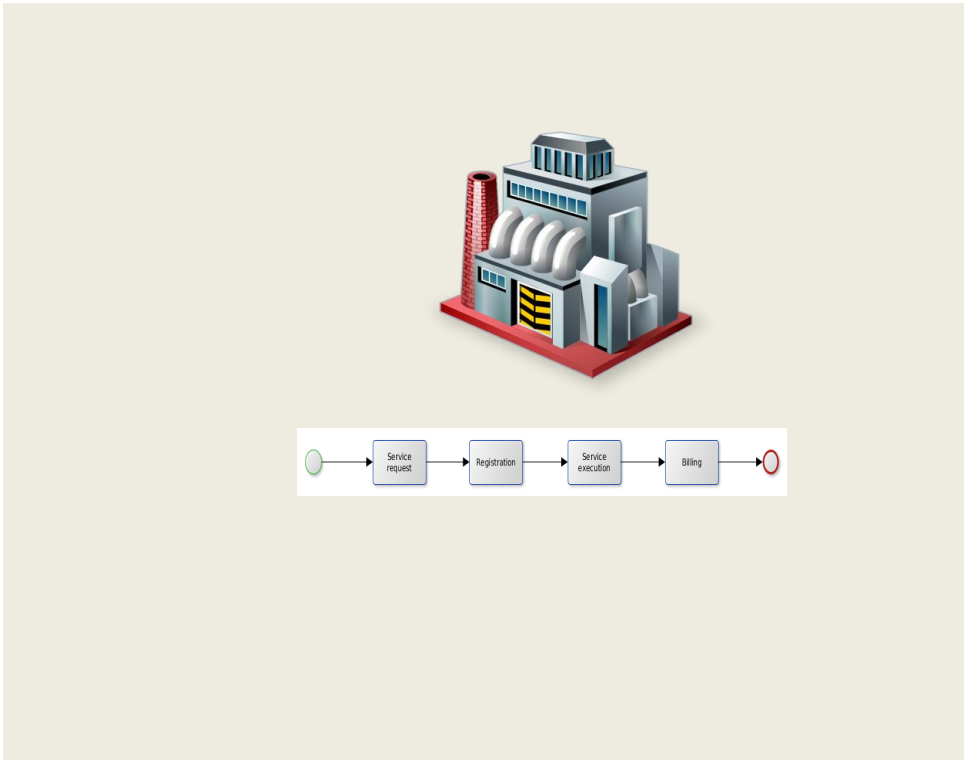
AC ensures that only the intended people can access security-classified data and that these intended users are only given the level of access required to accomplish their tasks



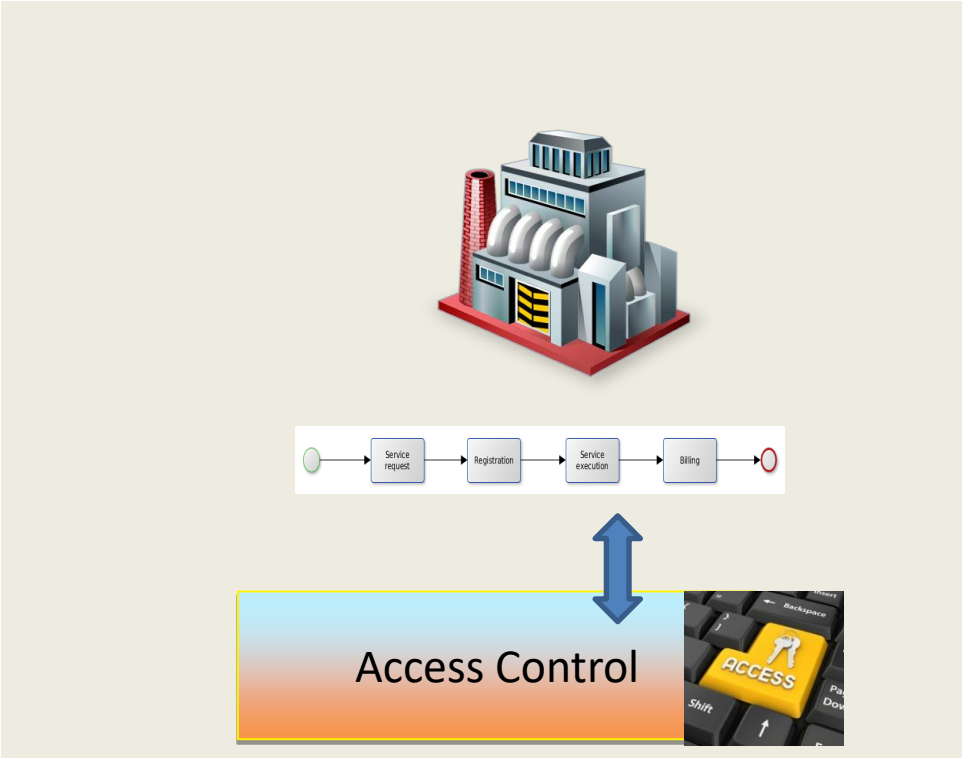
BPMN™

XACML OASIS Advancing open standards for the information society
www.oasis-open.org

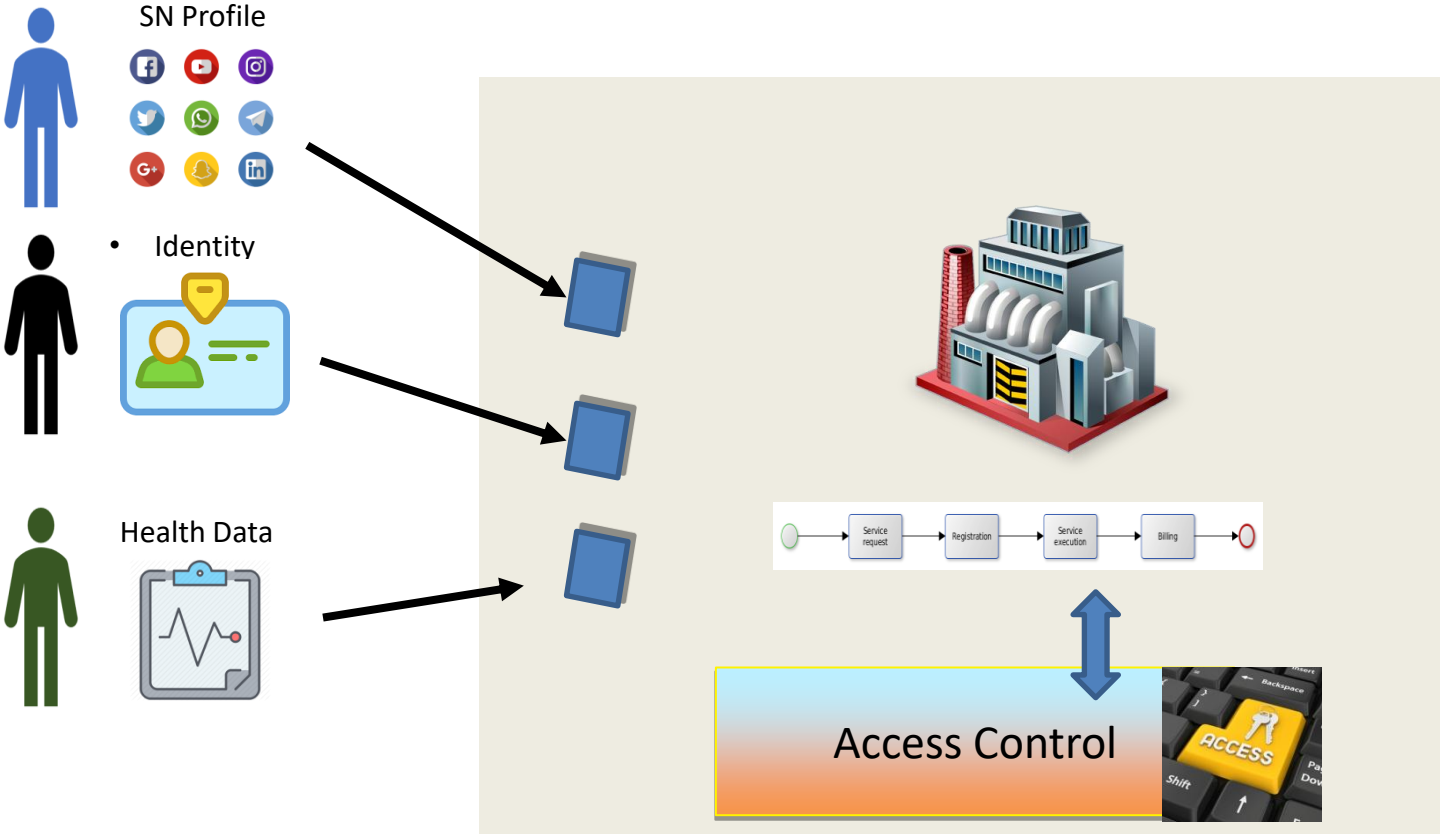
BP-based Access Control for GDPR



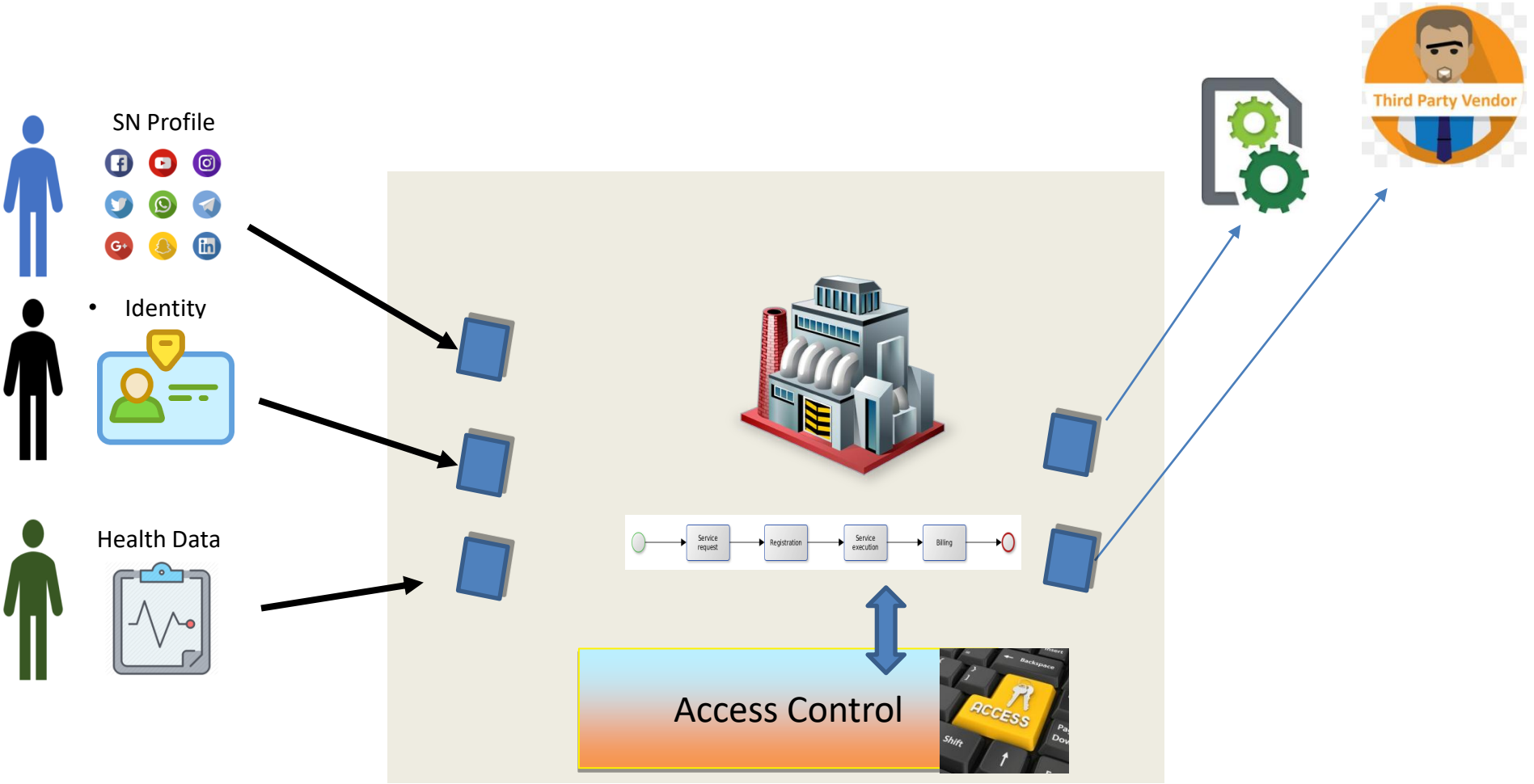
BP-based Access Control for GDPR



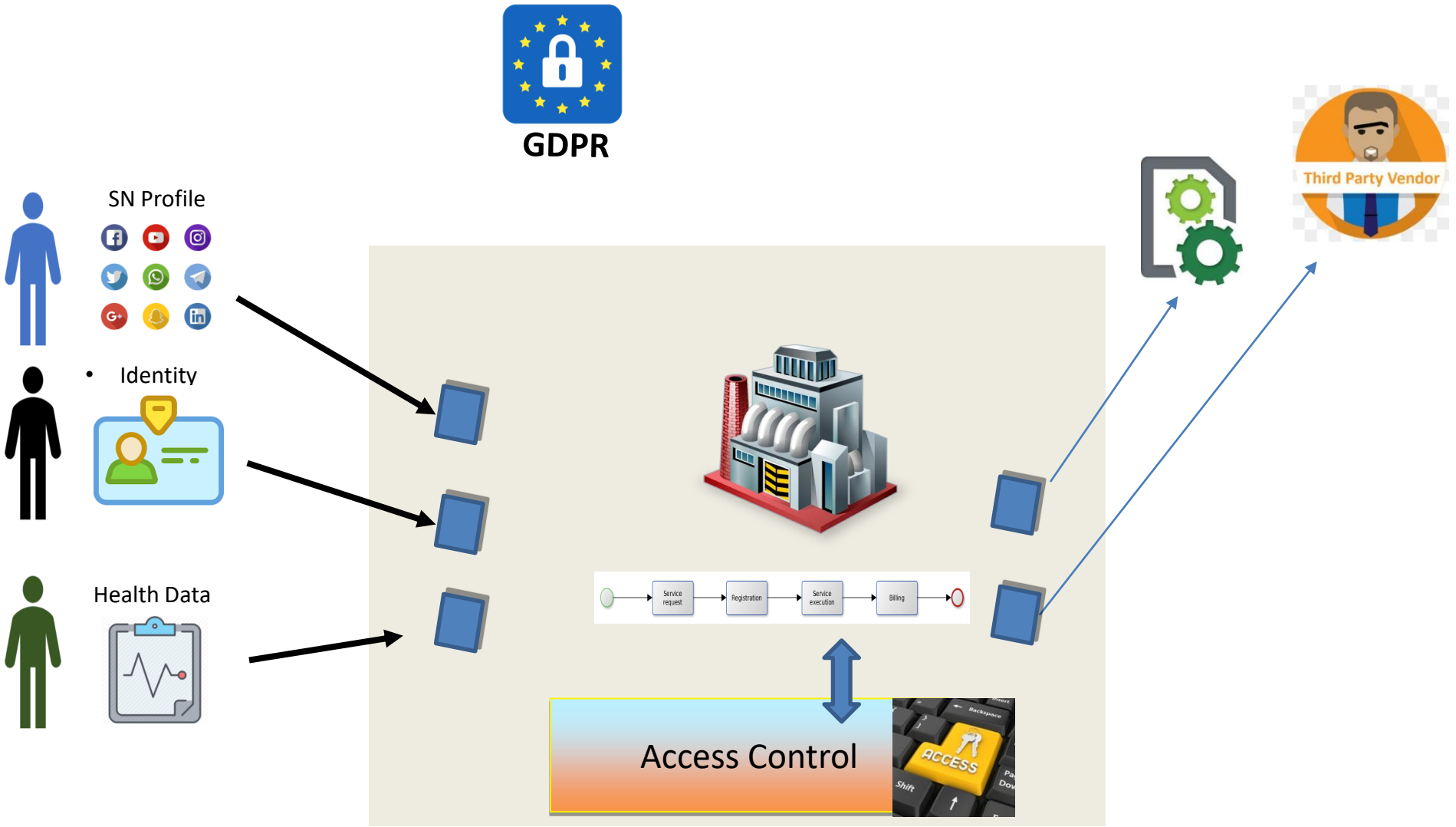
BP-based Access Control for GDPR



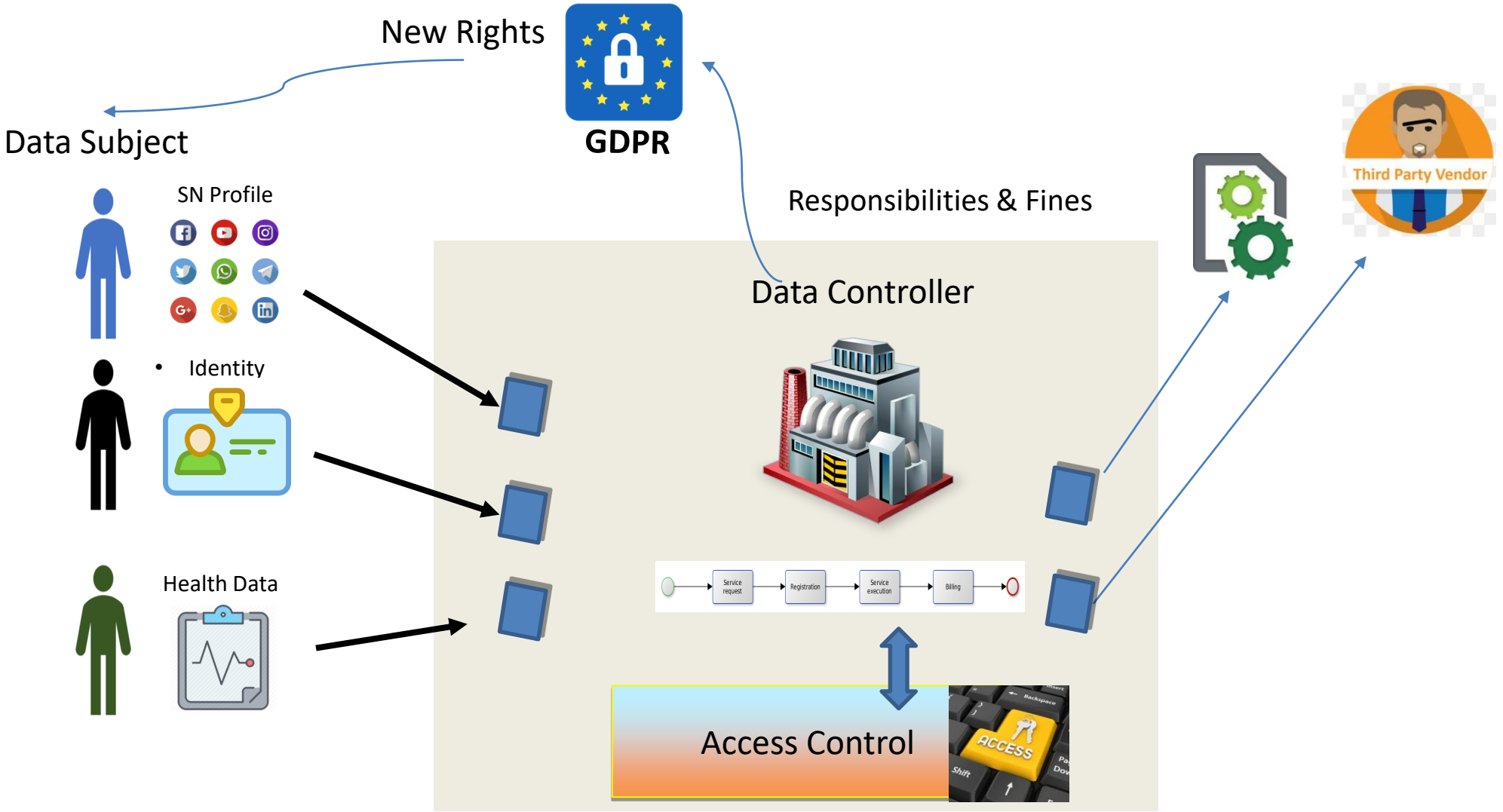
BP-based Access Control for GDPR



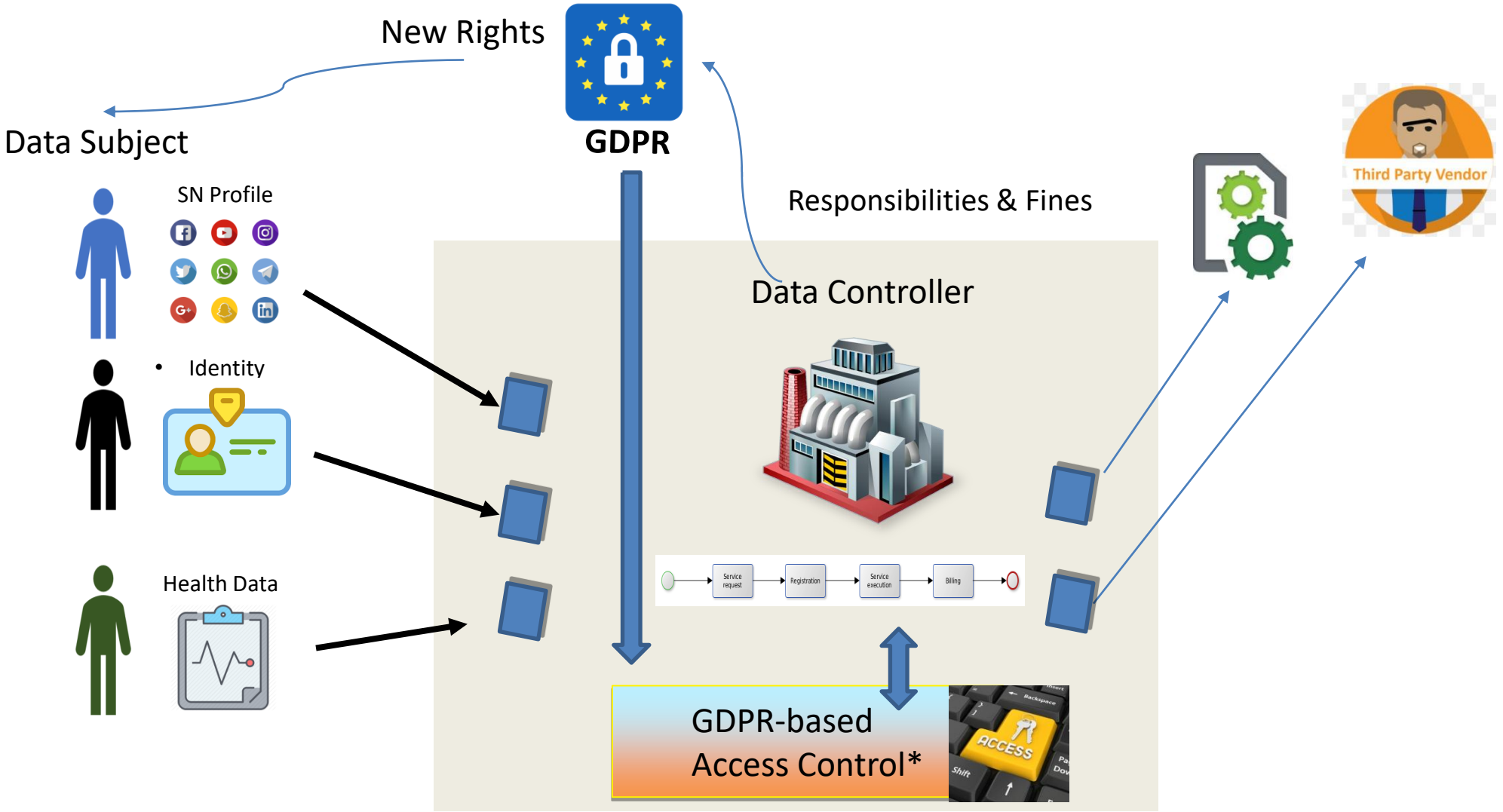
BP-based Access Control for GDPR



BP-based Access Control for GDPR

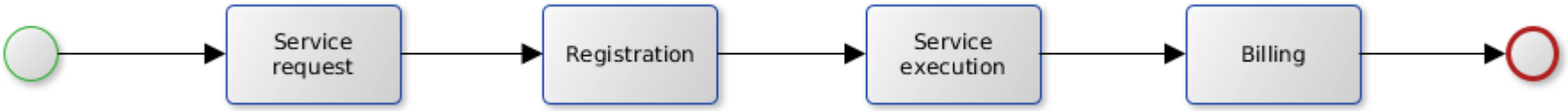


BP-based Access Control for GDPR



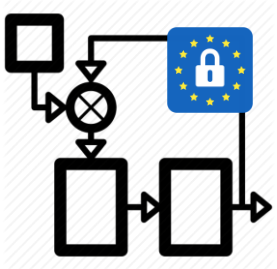
Integrating AC and BP for GDPR Presumption of Compliance

Define Use Cases

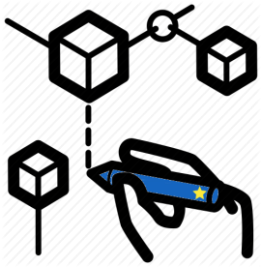


Possible scenario

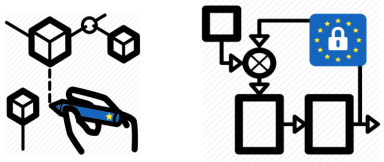
In case of already exiting BP, leverage the business process to be compliant with the GDPR



Provide facilities to model business process compliant with the GDPR



Gather authorization requirements

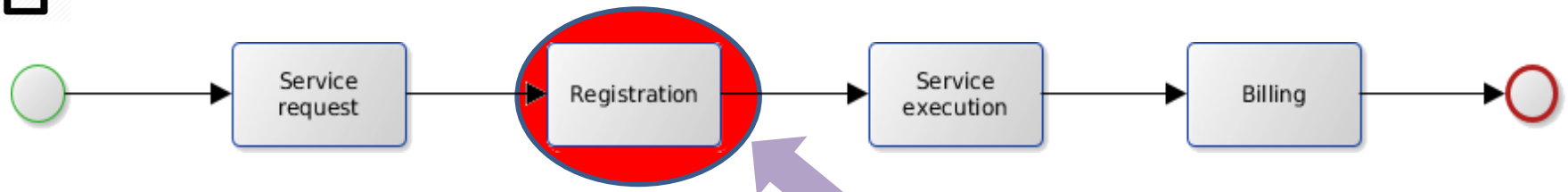


Gather all the authorization and business requirements and the sources they come from.

Expressed in terms of statements or natural language authorization policies

Identify required attributes

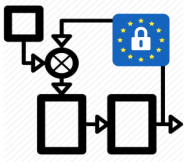
Scenario 1 – already exiting BP

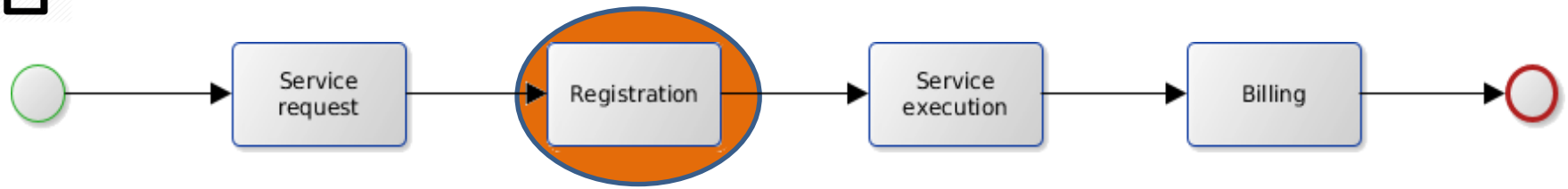


Extend/substitute BP activities with GDPR compliant ones

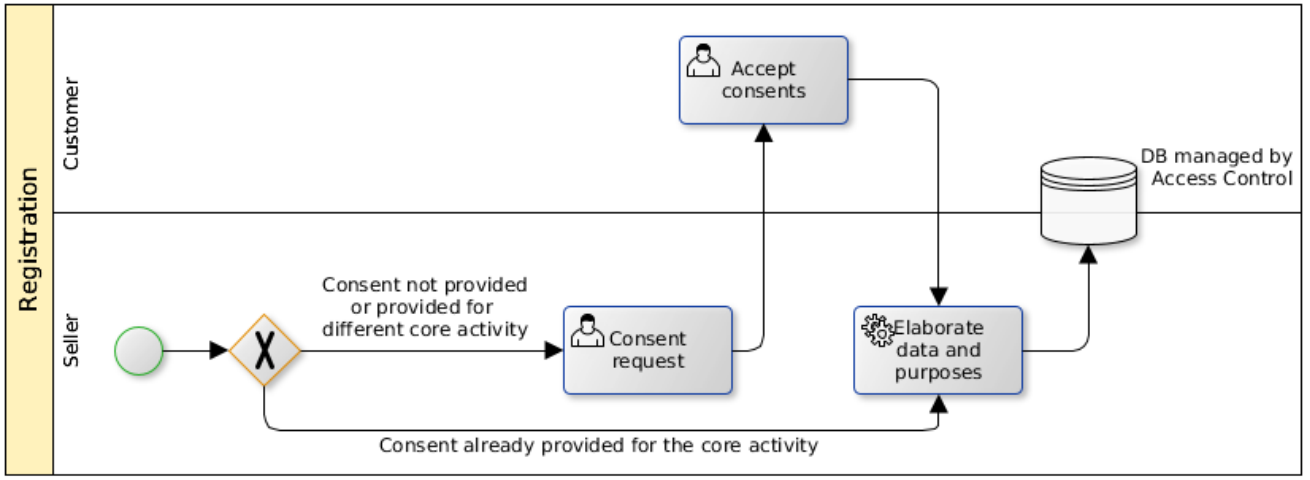
- pre-defined sets of sub-processes are provided for the different environments
- the sub-processes include specific activities allow the integration with GDPR-based access control systems

Identify required attributes



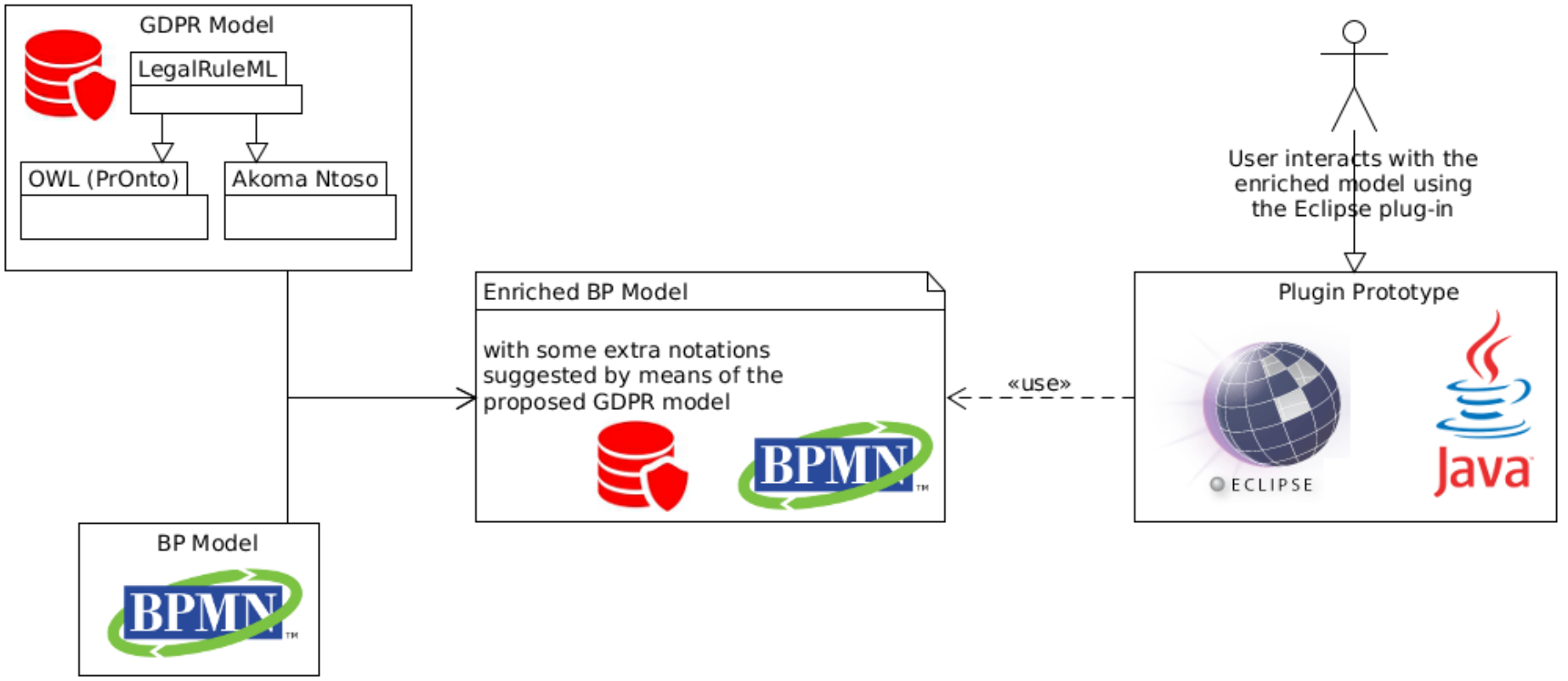


Tasks inception



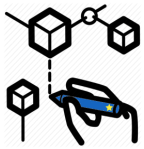
Identify required attributes

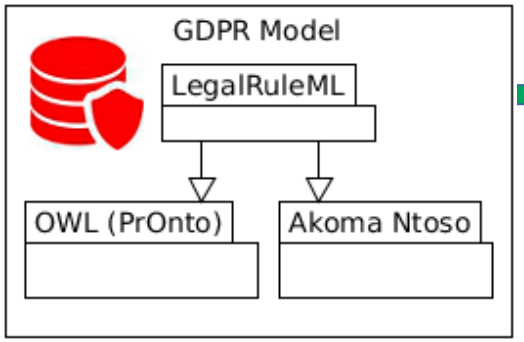
Scenario 2 – model business process compliant with the GDPR



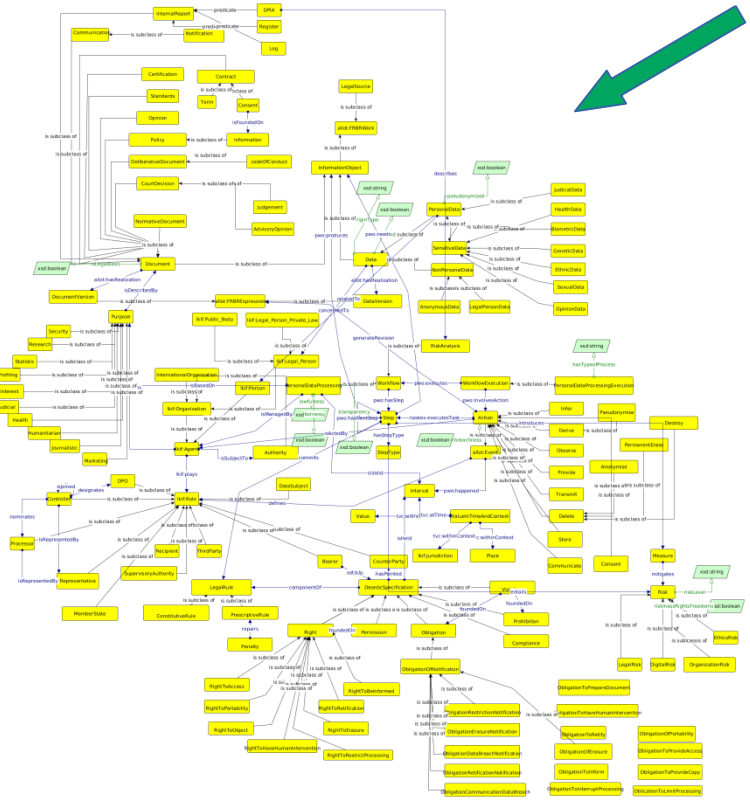
https://github.com/guerret/lu.uni.eclipse.bpmn2

Details about GDPR Model



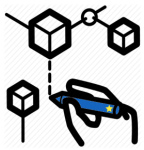



```
<lrml:LegalReferences type="legislative">
  <lrml:LegalReference refersTo="gdprC2A5P1p1ref" refID="GDPR:art_5__para_1
  <lrml:LegalReference refersTo="gdprC2A5P1p2ref" refID="GDPR:art_5__para_1
  <lrml:LegalReference refersTo="gdprC2A5P1p3ref" refID="GDPR:art_5__para_1
  <lrml:LegalReference refersTo="gdprC2A5P1p4ref" refID="GDPR:art_5__para_1
  <lrml:LegalReference refersTo="gdprC2A5P1p5ref" refID="GDPR:art_5__para_1
  <lrml:LegalReference refersTo="gdprC2A5P1p6ref" refID="GDPR:art_5__para_1
  <lrml:LegalReference refersTo="gdprC2A6P1p1ref" refID="GDPR:art_6__para_1
  <lrml:LegalReference refersTo="gdprC2A6P1p2ref" refID="GDPR:art_6__para_1
  <lrml:LegalReference refersTo="gdprC2A6P1p3ref" refID="GDPR:art_6__para_1
  <lrml:LegalReference refersTo="gdprC2A6P1p4ref" refID="GDPR:art_6__para_1
  <lrml:LegalReference refersTo="gdprC2A6P1p5ref" refID="GDPR:art_6__para_1
  <lrml:LegalReference refersTo="gdprC2A6P1p6ref" refID="GDPR:art_6__para_1
  <lrml:LegalReference refersTo="gdprC2A6P4ref" refID="GDPR:art_6__para_4"
  <lrml:LegalReference refersTo="gdprC2A7P1ref" refID="GDPR:art_7__para_1"
```

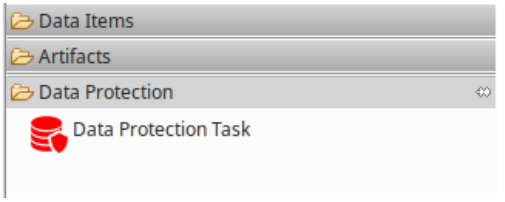


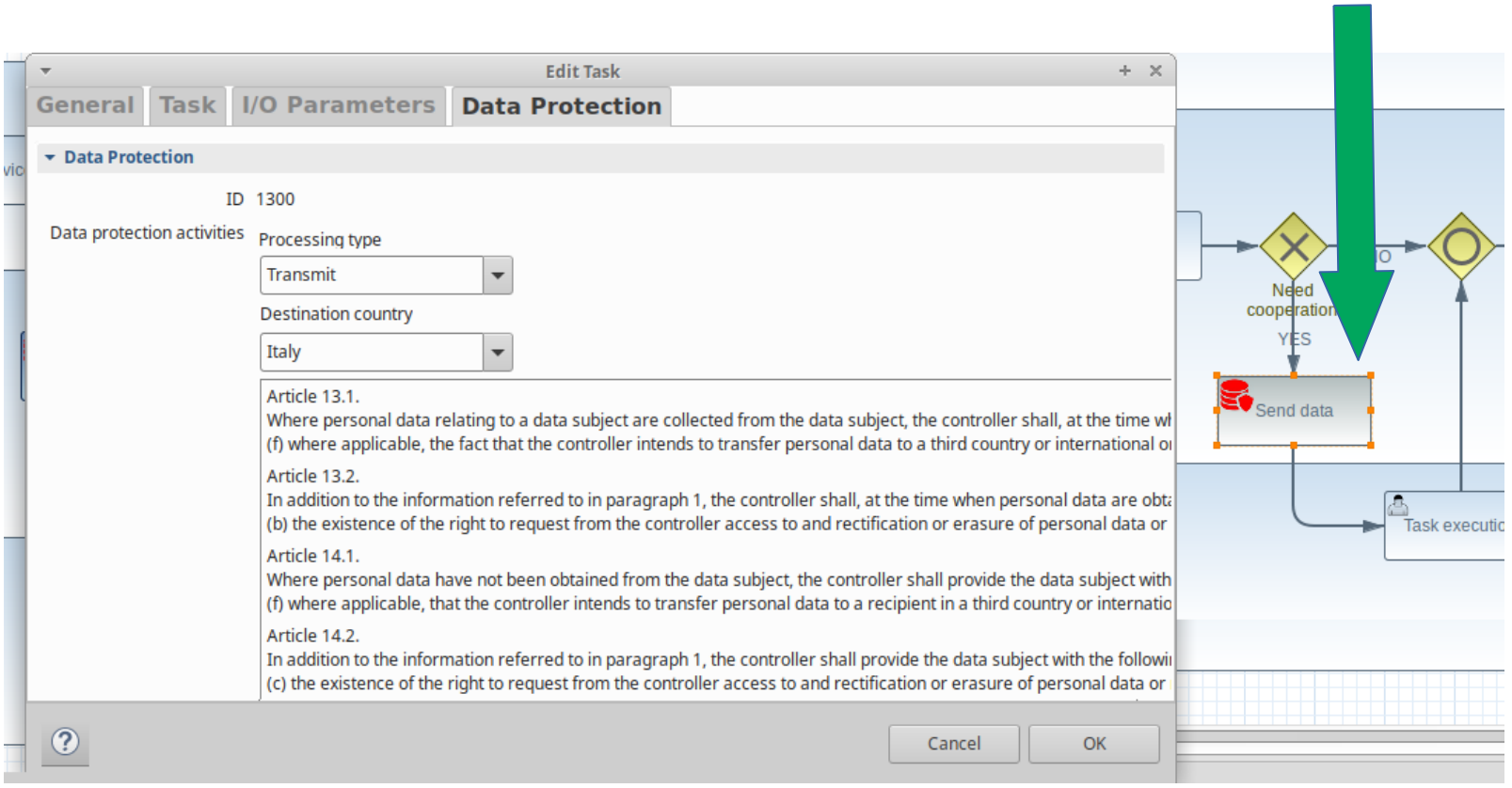
```
    <num>2.</num>
    <content eId="art_6__para_2__content">
        <p>Member States may maintain or introduce more specific provisions to adapt the application
            <ref href="/akn/eu/act/2017-12-12/!main/#paragraph.1" eId="ref_30" wId="content__ref_30">
        </p>
    </content>
</paragraph>
<paragraph eId="art_6__para_3">
    <num>3.</num>
        <list eId="art_6__para_3__content__list_1">
            <intro><p>The basis for the processing referred to in point (c) and (e) of
                <ref href="/akn/eu/act/2017-12-12/!main/#paragraph.1" eId="ref_31">paragraph 1</ref>
            </p></intro>
            <point eId="art_6__para_3__content__list_1__point_a">
                <num>(a)</num><content>
                <p>Union law; or</p></content>
            </point>
            <point eId="art_6__para_3__content__list_1__point_b">
                <num>(b)</num><content>
                <p>Member State law to which the controller is subject.
                    <eol/>The purpose of the processing shall be determined in that legal basis or, as
                    <ref href="/akn/eu/act/2017-12-12/!main/#paragraph.1" eId="ref_32">paragraph 1</re
                </p></content>
            </point>
        </list>
</paragraph>
<paragraph eId="art_6__para_4">
    <num>4.</num>
        <list eId="art_6__para_4__content__list_1">
            <intro><p>Where the processing for a purpose other than that for which the personal data ha
                <ref href="/akn/eu/act/2017-12-12/!main/#article.23" eId="ref_33">Article 23</ref>(1),
            </p></intro>
            <point eId="art_6__para_4__content__list_1__point_a">
                <num>(a)</num><content>
                <p>any link between the purposes for which the personal data have been collected and t
            </point>
            <point eId="art_6__para_4__content__list_1__point_b">
                <num>(b)</num><content>
                <p>the context in which the personal data have been collected, in particular regarding
            </point>
```

Eclipse prototype

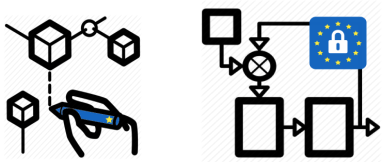


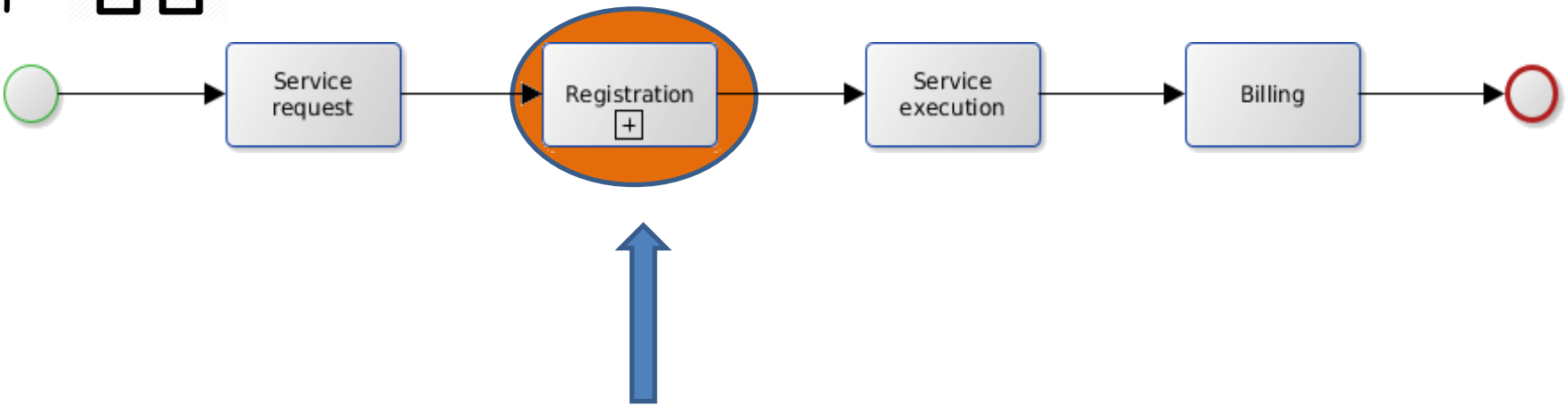
Plugin Prototype

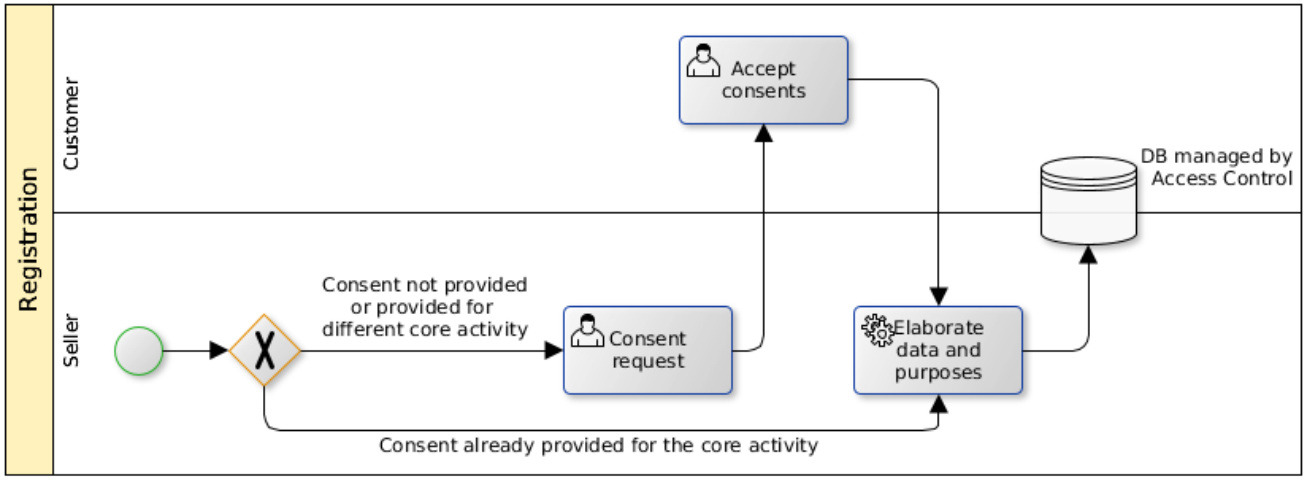




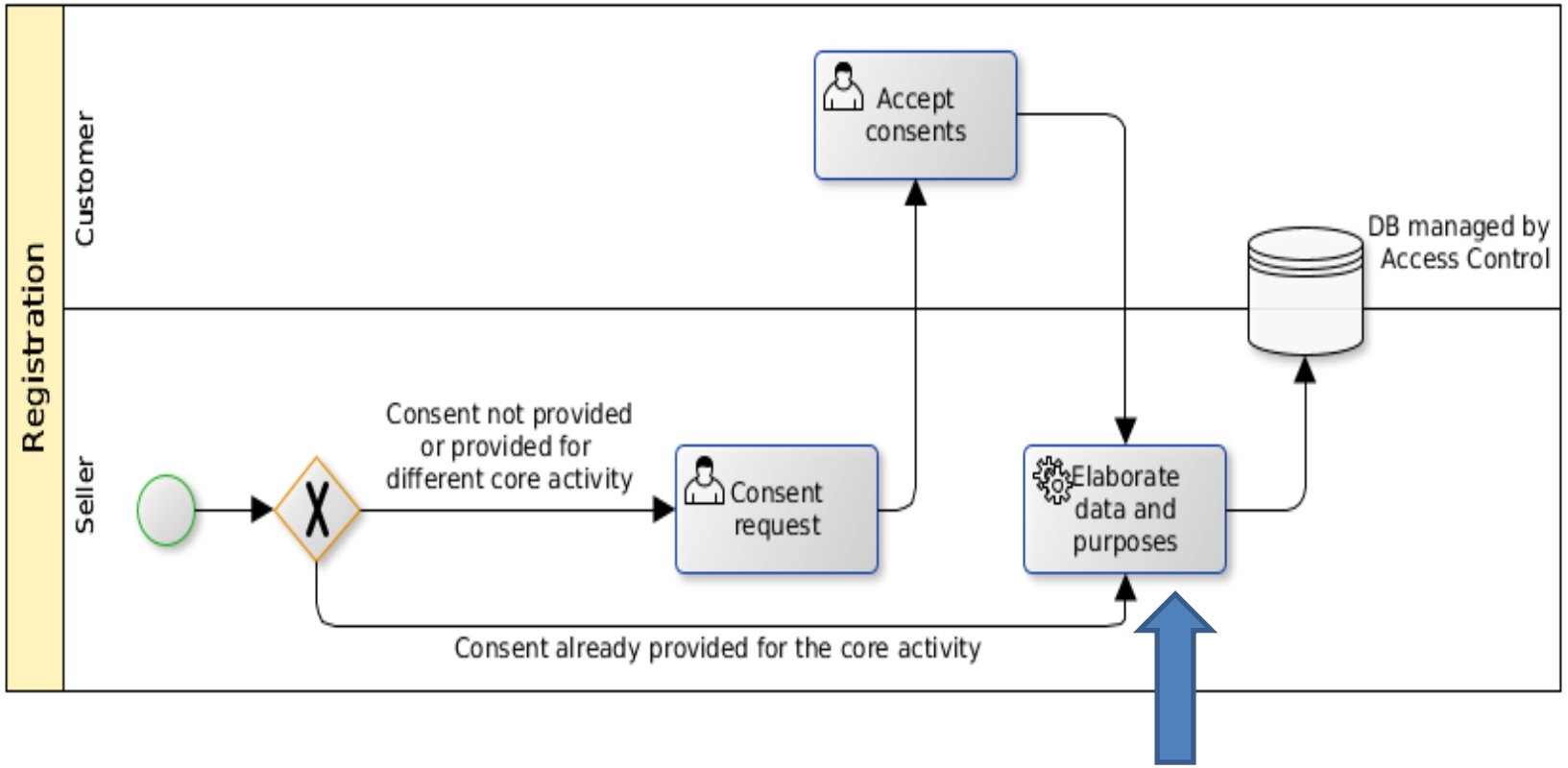
Identify required attributes





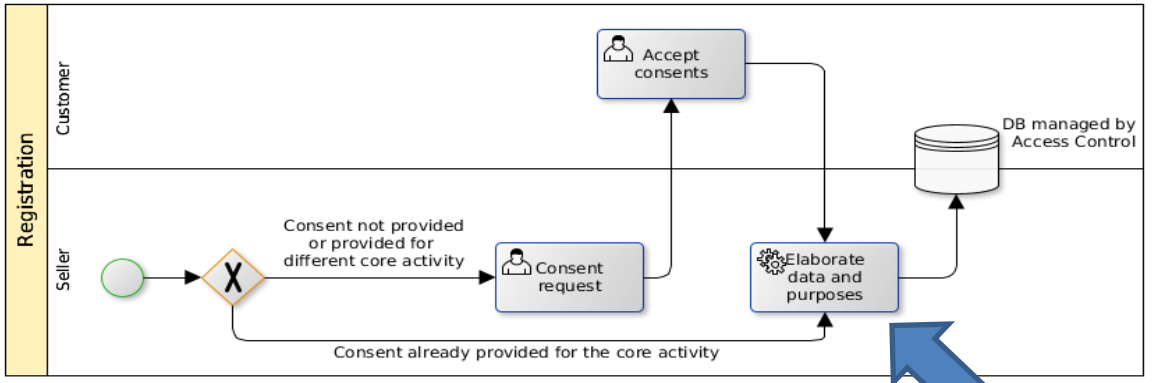


Author the authorization policies



Transform the collected GDPR requirements, data and their purposes into machine-interpretable statements, so as to eliminate any ambiguity introduced by natural language

Author the authorization policies



Consent Request

FirstName	
LastName	
PhoneNumber	
E-mailAddress	
OptionalPurposes	Newsletter, Target Marketing
PrimaryPurpose	Core Activity

Consent Response

FirstName	Eda
LastName	Marchetti
PhoneNumber	+39 1234567899
E-mailAddress	eda.marchetti@isti.cnr.it
OptionalPurposes	Target Marketing
PrimaryPurpose	Core Activity

Consent Response

FirstName	Eda
LastName	Marchetti
PhoneNumber	+39 1234567899
E-mailAddress	eda.marchetti@isti.cnr.it
OptionalPurposes	Target Marketing
PrimaryPurpose	Core Activity

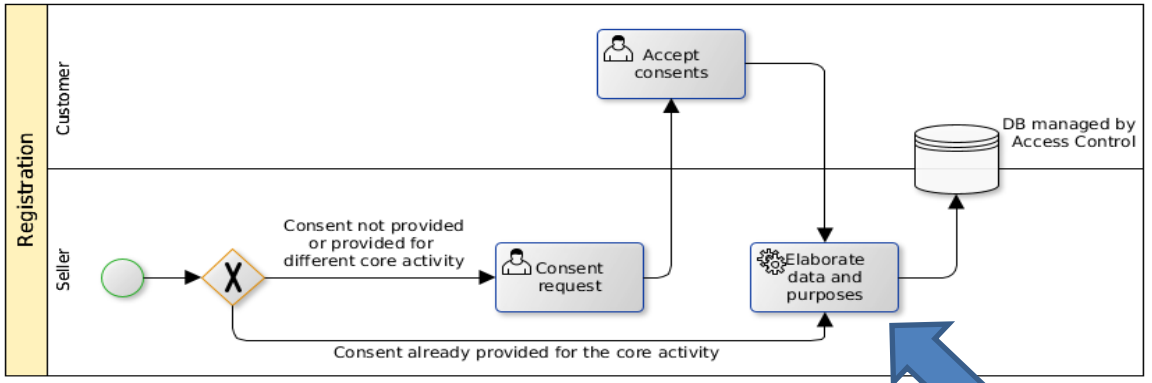
Added Attributes

Duration	30 Days
StartingDate	2018.11.14

SPECIFY THE PURPOSES

a. b. c.

Author the authorization policies



Consent Request

FirstName	
LastName	
PhoneNumber	
E-mailAddress	
OptionalPurposes	Newsletter, Target Marketing
PrimaryPurpose	Core Activity

Consent Response

FirstName	Eda
LastName	Marchetti
PhoneNumber	+39 1234567899
E-mailAddress	eda.marchetti@isti.cnr.it
OptionalPurposes	Target Marketing
PrimaryPurpose	Core Activity

Consent Response

FirstName	Eda
LastName	Marchetti
PhoneNumber	+39 1234567899
E-mailAddress	eda.marchetti@isti.cnr.it
OptionalPurposes	Target Marketing
PrimaryPurpose	Core Activity

Added Attributes

Duration	30 Days
StartingDate	2018.11.14

SPECIFY IMPLICIT ATTRIBUTES

a. b. c.

Deploy the architecture

Deploy the architecture: list of XACML policies encoding the GDPR principle are specified and deployed into the architecture

Policy	root element rule-combining-algorithm:first-applicable permit-overrides
Target	Sample Policy rules the access to the attributes of the *Customer*.
AnyOf	Or Operator
AllOf	resource-attributes = {Eda, Marchetti, +39 1234567899, eda.marchetti@isti.cnr.it}
Rule	RuleId = rule1, Effect = Permit
Target	The *Seller* can perform any action for the *Core Activity* and / or *Target Marketing* purposes within 30 days starting from the *StartingDate*.
AnyOf	Or Operator
AllOf	PrimaryPurpose = Core Activity
AllOf	OptionalPurpose = Target Marketing
Condition	30 ≤ CurrentDate - StartingDate
Rule	default: deny all, which is not allowed explicitly. RuleId = rule2, Effect = Deny

Consent Request

FirstName	
LastName	
PhoneNumber	
E-mailAddress	
OptionalPurposes	Newsletter, Target Marketing
PrimaryPurpose	Core Activity

a.

Consent Response

FirstName	Eda
LastName	Marchetti
PhoneNumber	+39 1234567899
E-mailAddress	eda.marchetti@isti.cnr.it
OptionalPurposes	Target Marketing
PrimaryPurpose	Core Activity

b.

Consent Response

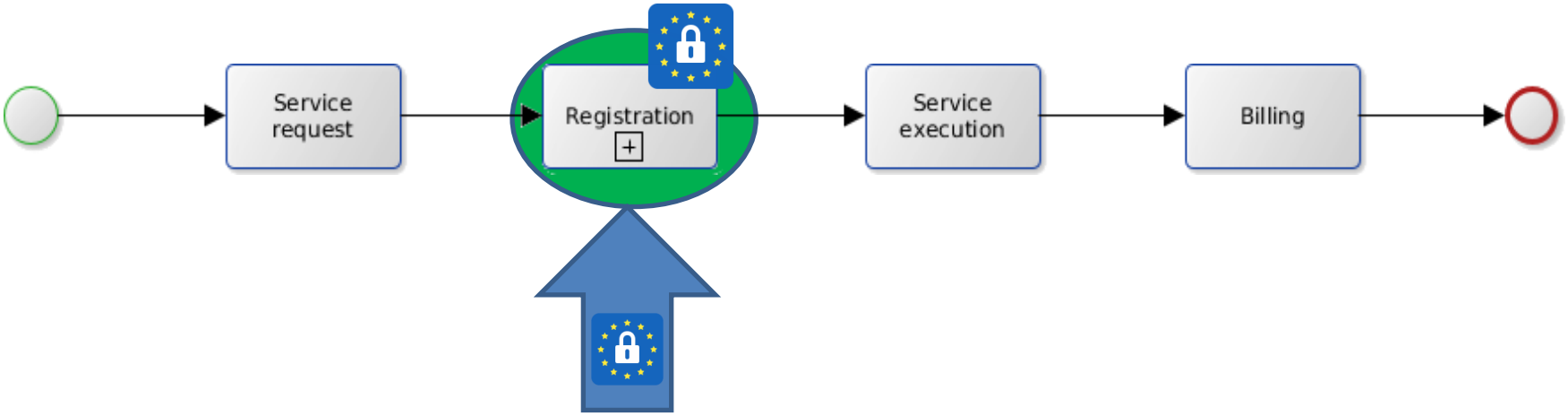
FirstName	Eda
LastName	Marchetti
PhoneNumber	+39 1234567899
E-mailAddress	eda.marchetti@isti.cnr.it
OptionalPurposes	Target Marketing
PrimaryPurpose	Core Activity

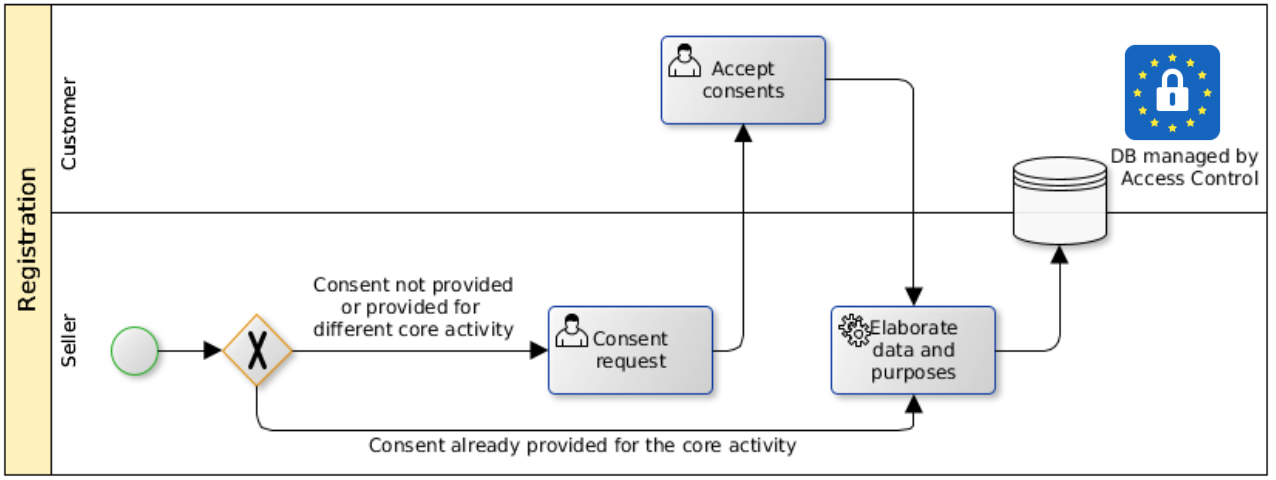
Added Attributes

Duration	30 Days
StartingDate	2018.11.14

c.

Final integration





Where are we?


IDENTIFY REQUIRED ATTRIBUTES
GATHER AUTHORIZATION REQUIREMENTS
AUTHOR THE AUTHORIZATION POLICIES
DEFINE THE USE CASE
DEPLOY THE ARCHITECTURE