The SPECIAL Policy Log Vocabulary

A vocabulary for privacy-aware logs, transparency and compliance

Javier D. Fernández, Piero Bonatti, Wouter Dullaert, Sabrina Kirrane, Uros Milosevic, Axel Polleres

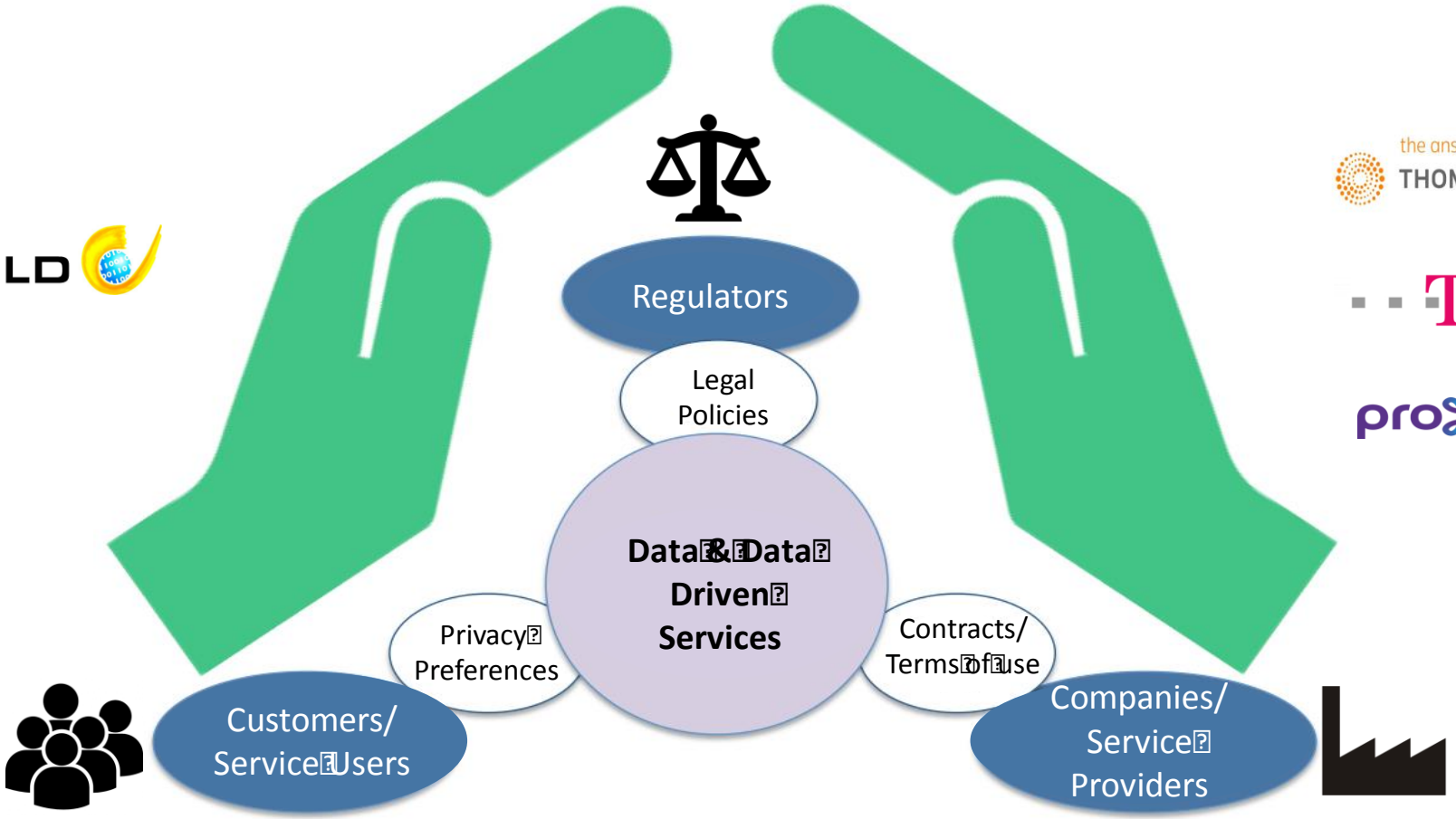
W3C Workshop on Privacy and Linked Data
18/04/2018

European Commission

Horizon 2020
European Union funding
for Research & Innovation

SPECIAL Overview

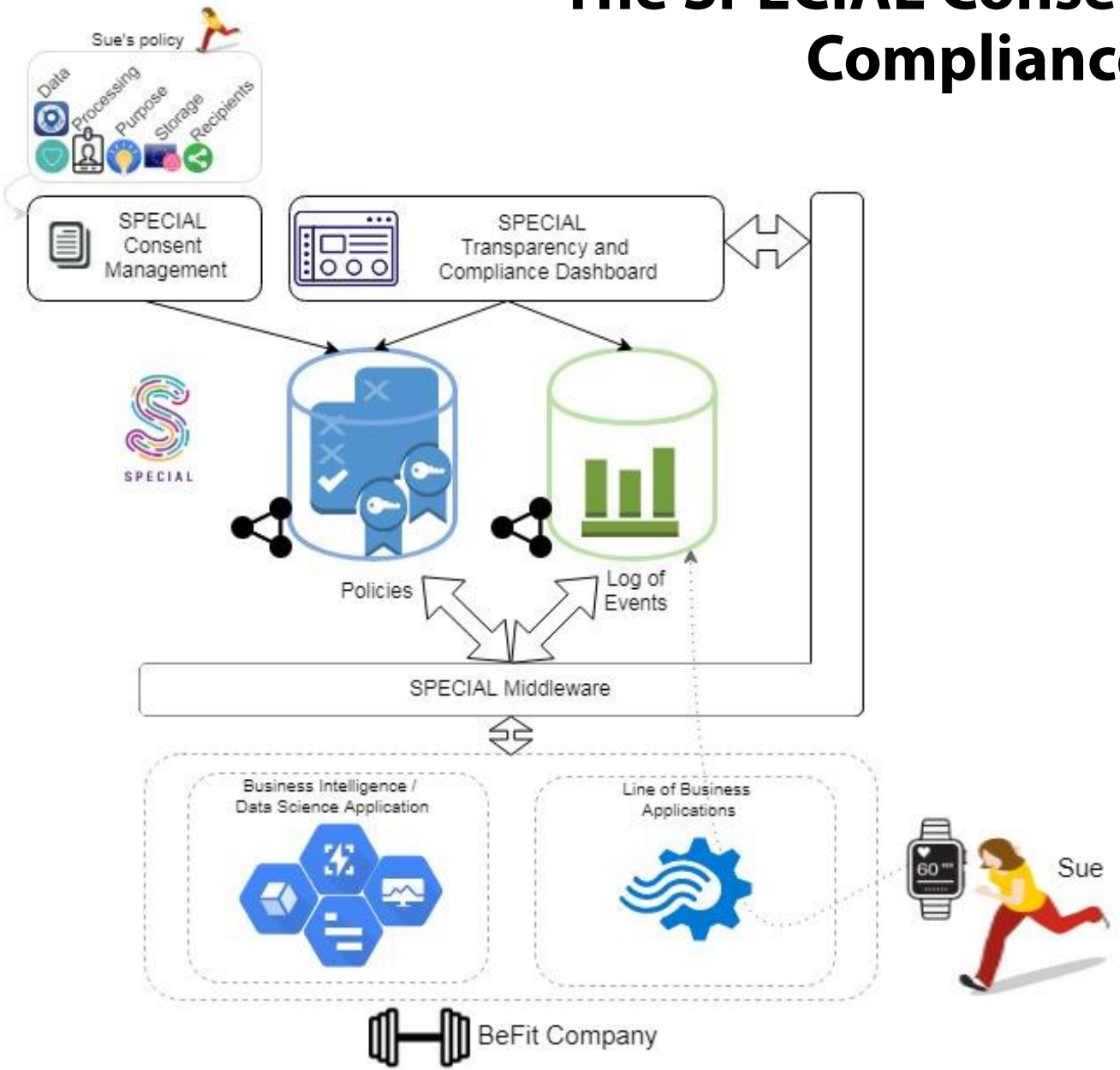
Aims



SPECIAL Overview
Objectives

- Policy management framework
  - ❖ Gives **users control** of their personal data
  - ❖ Represents **access/usage policies** and **legislative requirements** in a **machine readable format**
- **Transparency and compliance framework**
  - ❖ **Provides information on how data is processed and with whom it is shared**
  - ❖ **Allows data subjects to take corrective action**
- Scalable policy-aware Linked Data architecture
  - ❖ Build on top of the Big Data Europe (BDE) platform **scalability and elasticity mechanisms**
  - ❖ Extended BDE with **robust policy, transparency** and **compliance protocols**

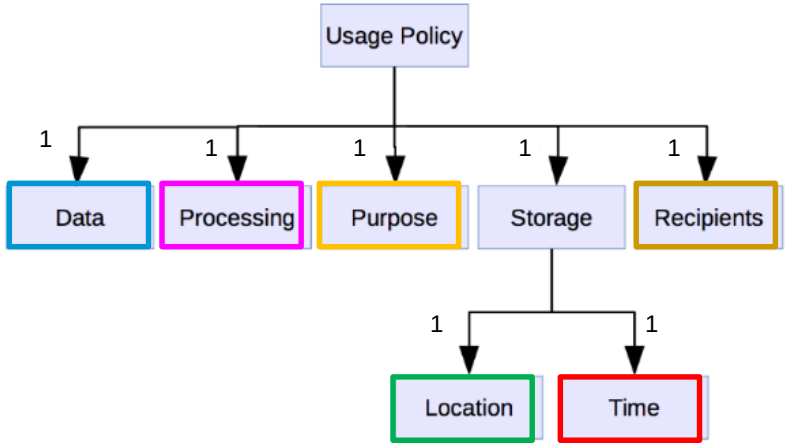
The SPECIAL Consent, Transparency and Compliance framework



Privacy policy formalization

- Record **usage policies**
- SPECIAL is releasing the SPECIAL policy language
  - Based on OWL EL

“**Heart rate** and **location data** are **collected** and **analysed** to create a **user profile** for the purpose of issuing **recommendations**. Profiles are stored **indefinitely** in the **EU** by the data controller and released to **third parties**.”




```
EquivalentClasses(<http://company.org/consents/Recommendations>
ObjectIntersectionOf(
        ObjectSomeValuesFrom( spl:hasData
                ObjectUnionOf(
                ex:HeartRate svd:Location ))
        ObjectSomeValueFrom( spl:hasProcessing
                        ObjectIntersectionOf(svpr:Collect svpr:Analyze px:Profiling ))
        ObjectSomeValueFrom( spl:hasPurpose ex:Recommendation)
        ObjectSomeValueFrom( spl:hasStorage
                ObjectIntersectionOf(
                        ObjectSomeValuesFrom( spl:hasLocation
                                ObjectIntersectionOf( svl:OurServers svl:EU ))
                        DataSomeValuesFrom( spl:durationInDays
                                DatatypeRestriction( xsd:integer
                                xsd:mininclusive "0"^^xsd:integer ))))
        ObjectSomeValueFrom( spl:hasRecipient svr:AnyRecipient )))
```

```
ex:Recommendation rdfs:subClassOf svpu:Marketing .
```

Transparency framework

- Record **data processing and sharing events**
- We have developed a vocabulary for the logs (SPLOG)
  - http://purl.org/specialprivacy/splog

Unofficial Draft

TABLE OF CONTENTS

1. **Introduction**
1.1 What is a Usage Policy?
1.2 Audience and scope
1.3 Document conventions and namespaces

2. **Conformance**

3. **The SPECIAL's Usage Policy Language**
3.1 Basic Usage Policies
3.2 General Usage Policies
3.3 Storage Expressions

4. **Compliance Checking**

5. **SPECIAL's Usage Policy Language Grammar**

6. **Acknowledgements**

A. **References**
A.1 Normative references
A.2 Informative references

ReSpec

The SPECIAL Usage Policy Language

version 0.1

Unofficial Draft 06 April 2018

Editor:
Javier D. Fernández (Vienna University of Economics and Bu

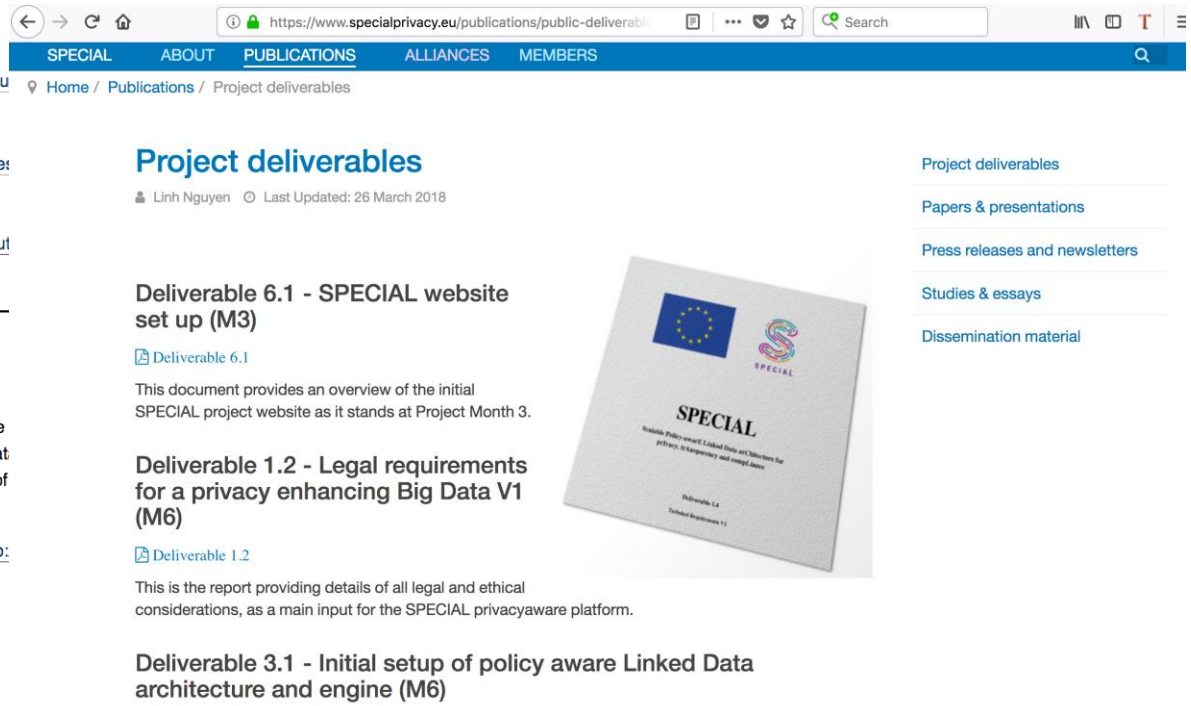
Authors:
Piero Bonatti (Università di Napoli Federico II)
Sabrina Kirrane (Vienna University of Economics and Busines
Iliana Mineva Petrova (Università di Napoli Federico II)
Luigi Sauro (Università di Napoli Federico II)
Eva Schlehahn (Unabhängies Landeszentrum für Datenschut

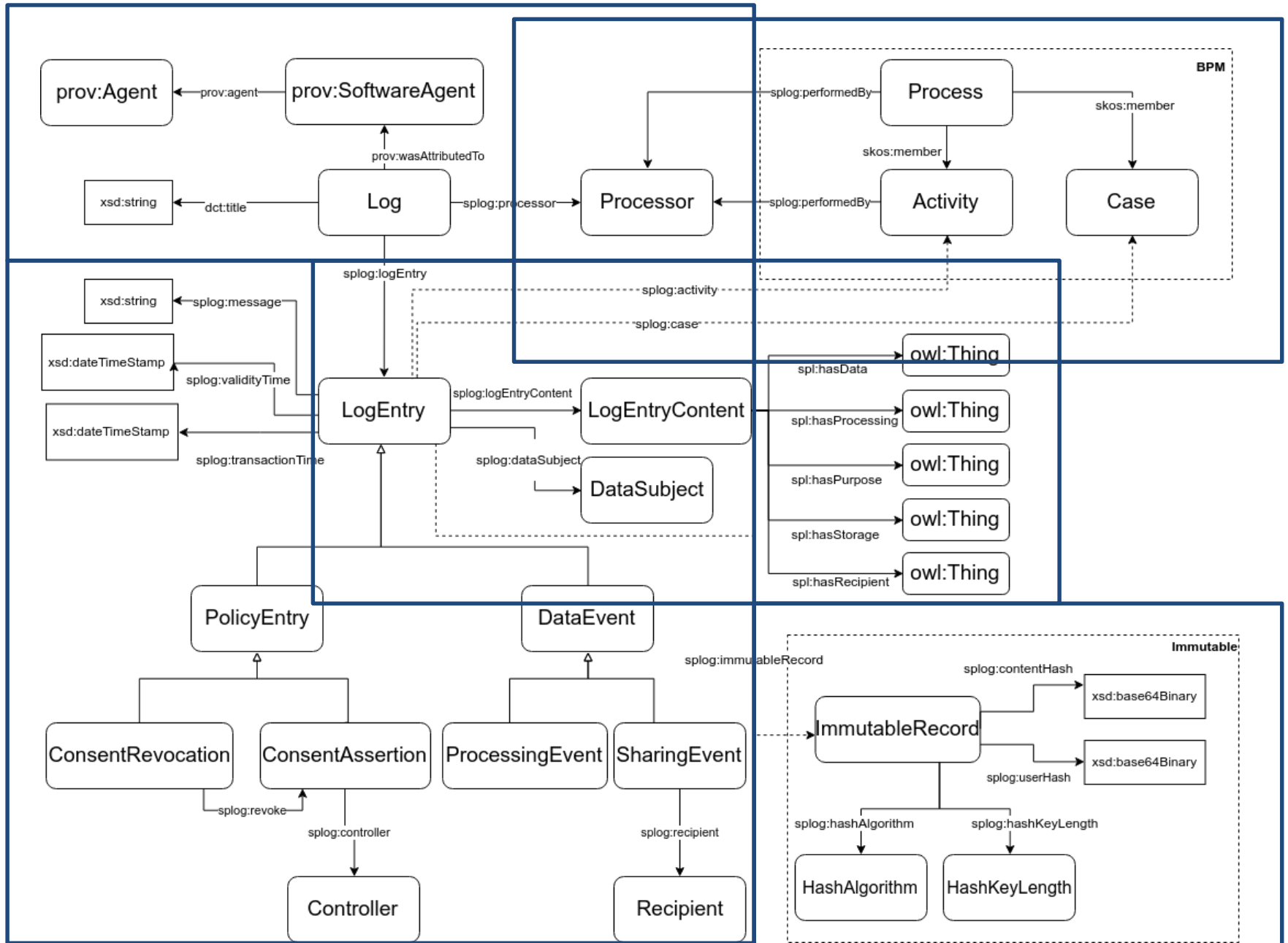
This document is licensed under a Creative Commons Attribution 3.0 License.

Abstract

This document specifies usage policy language of SPECIAL. The
both the data subjects' consent and the data usage policies of dat
able by a computer, so as to automatically verify that the usage of
consent.

The ontology defined in this document is publicly available at http:
policy.




prov:Agent
prov:agent
prov:SoftwareAgent
prov:wasAttributedTo
xsd:string
dct:title
Log
splog:processor
Processor
BPM
splog:performedBy
Process
skos:member
skos:member
splog:performedBy
Activity
Case
splog:logEntry
splog:activity
splog:case
xsd:string
splog:message
xsd:dateTimeStamp
splog:validityTime
LogEntry
splog:logEntryContent
LogEntryContent
xsd:dateTimeStamp
splog:transactionTime
splog:dataSubject
DataSubject
spl:hasData
owl:Thing
spl:hasProcessing
owl:Thing
spl:hasPurpose
owl:Thing
spl:hasStorage
owl:Thing
spl:hasRecipient
owl:Thing
PolicyEntry
DataEvent
splog:immutableRecord
Immutable
splog:contentHash
xsd:base64Binary
ImmutableRecord
xsd:base64Binary
splog:userHash
ConsentRevocation
ConsentAssertion
ProcessingEvent
SharingEvent
splog:hashAlgorithm
splog:hashKeyLength
splog:revoke
splog:controller
splog:recipient
HashAlgorithm
HashKeyLength
Controller
Recipient

Transparency framework

- Record **data processing and sharing events**
- We have developed a vocabulary for the logs (SPLOG)
  - http://purl.org/specialprivacy/splog

befit:BeFitLog a splog:Log;

dct:title	"Log of BeFitDatabaseEurope"@en;
dct:description	"This contains events on BeFitDatabaseEurope tracking devices geo-located in Europe"@en;
dct:issued	"2018-02-14"^^xsd:date;
prov:wasAttributedTo	befit:BeFitDatabaseEurope ;
splog:processor	befit:Us .

Transparency framework

- Record **data processing and sharing events**
- We have developed a vocabulary for the logs (SPLOG)
  - http://purl.org/specialprivacy/splog

befit:entry3918 a splog:ProcessingEvent;

dct:title	"Collection of new device position"@en;
splog:dataSubject	befit:Sue ;
dct:description	"We collected a new position of your BeFit device in our database in Europe"@en;
splog:transactionTime	"2018-01-10T13:20:50Z"^^xsd:dateTimeStamp;
splog:validityTime	"2018-01-10T13:20:00Z"^^xsd:dateTimeStamp;
splog:message	"Tracking position by GPS... collected!" ;
splog:eventContent	befit:content3918 ;

Transparency framework

- Record **data processing and sharing events**
- We have developed a vocabulary for the logs (SPLOG)
  - http://purl.org/specialprivacy/splog

befit:content3918 a splog:LogEntryContent;
dct:description "Location data are collected by a BeFit device only for the health purpose of the service"@en;
spl:hasData svd:Location;
spl:hasProcessing befit:SensorGathering;
spl:hasPurpose befit:HealthTracking;
spl:hasStorage [has:location svl:OurServers];
spl:hasRecipient [a svr:Ours].

befit:SensorGathering rdfs:subClassOf svpr:Collect .
befit:HealthTracking rdfs:subClassOf svpu:Health .

Transparency framework

- Record **data processing and sharing events**
- We have developed a vocabulary for the logs (SPLOG)
  - http://purl.org/specialprivacy/splog
- We have a running prototype (ESWC 2018)

Discussion

- lack of specific and standard **vocabularies** for representing **privacy-related events**
- It should be possible to describe the event content at different **granularities**
    - from a simple **taxonomy** (stating the type of data, processing, etc.), to the most fine-grained description of the **actual data** associated to the event;
- **Interoperability/standard APIs**
    - different systems within a company and/or different companies

The SPECIAL Policy Log Vocabulary

A vocabulary for privacy-aware logs, transparency and compliance

Javier D. Fernández, Piero Bonatti, Wouter Dullaert, Sabrina Kirrane, Uros Milosevic, Axel Polleres

W3C Workshop on Privacy and Linked Data
18/04/2018

European Commission

Horizon 2020
European Union funding
for Research & Innovation