Formalization of the GDPR and of the Pilots' Policies

P.A. Bonatti, L. Ioffredo, G. Luongo, S. Mosi, I.M. Petrova, L. Sauro
CeRICT

SPECIAL REPORT – WP5-CeRICT-1 December 14, 2019

H2020-ICT-2016-2017, ICT-18-2016
Project No. 731601

Abstract

This technical report illustrates in detail the OWL2 artifacts (ontologies) that encode the business policies for the pilots, and the formalization of the GDPR. The report further shows the compliance checks that have been used to validate the formalization of the GDPR.

Contents

Chapter 1

Formalizing the GDPR

Here we extend – and where necessary modify – a previous version of the formalization of the GDPR, reported in D2.6. We have applied, when possible, the vocabularies recently published by the DPVCG community group of the W3C[1]. However, since the work reported here and DPVCG's activities have been carried out in parallel, the terms used in this report may be partially disaligned with the published vocabularies. Note also that most of the terms we propose in this report have been independently included in the vocabularies, with minor variations.

Recall that we are encoding the GDPR in OWL in such a way that a business policy BP complies with the GDPRs encoding ENC if and only if:

1. BP is not internally contradictory (i.e. not a subclass of owl:Nothing), and
2. SubClassOf(BP ENC) holds, that is, BP is a subclass of ENC.

This helps in understanding the formalization approach illustrated in the following sections.

1.1 Scope of the formalization

A use case concerning the automated support to checking the compliance of business policies with respect to the GDPR has been proposed by one of SPECIAL's industrial partners (Benedict Whittam-Smith, Thomson-Reuters/Refinitive). The goal of such compliance checks is validating business policies in terms of the mutual coherency of their properties, based on a formalization of the objective part of the GDPR.

The formalization covers only the aspects that concern controllers and processors, in terms of requirements on processing and obligations. The obligations and guidelines for the Union and Member States, and for the data protection authorities lie outside the scope of the formalization. This is because the tools for checking compliance with the GDPR are being designed primarily for controllers and processors, as a support to business process design and validation. The requirements in Chapter 3 of the GDPR

[1] https://www.w3.org/community/dpvcg/

(that concern the rights of the data subjects) are taken into account, since handling user rights requires controllers and processors to set up suitable business processes to meet the obligations posed by the regulation.

Given that SPECIAL's formalization of the GDPR is only a proof-of-concept, aimed at demonstrating the kind of automated validation checks that can be performed on business policies, we do not articulate in detail those requirements that cannot be checked, derived, or analyzed automatically, or that are always dealt with together, in a uniform way. In these cases, we lump together such requirements using a single, comprehensive term. However, we remark that in a concrete working environment it may be profitable to split such monolithic classes into finer-grained classes, that correspond to separate "boxes to be ticked" by human responsibles (indeed, such need has been expressed by the interested partner).

1.2 GDPR-related vocabulary terms

The GDPR places stronger constraints on some kinds of processing, that involve particular categories of data or particular purposes (cf. Art. 9 and 10, for example). Then it is necessary to introduce classes that formalize such data categories and purposes. In particular, the following new data categories are needed:[2]

```
PersonalData,
SensitiveData_as_per_Art9,                    (1.1)
SecurityMeasureData_as_per_Art10
```

These classes can be used in conjunction with classes like `Demographic` and `Location` in order to fully describe the nature and contents of the data. For example

```
ObjectIntersectionOf( SensitiveData_as_per_Art9
                      Demographic )
```

denotes the category of demographic data that are sensitive as per Art. 9. We will see concrete examples in Section 2.2 and 2.3.

Following the prescriptions of Art. 9, we futher introduce several data types that are considered to be sensitive by their nature:

```
Biometric, EthnicOrigin, Genetic
MedicalHealth, PhilosophicalBelief
PoliticalAffiliation, Race,                   (1.2)
ReligiousBelief
Sexual, TradeUnionMembership.
```

1.3 Modelling the GDPR requirements

The GDPR is organized in chapters that deal with lawfulness of processing, data subject rights, obligations of controllers and processors, and so on. SPECIAL's formalization

[2] Analogies of some of these classes have been included in DPVCG's vocabularies.

introduces a class for each of such "top-level" requirements that concerns the business policies of controllers and processors, and in particular for chapters 2, 3, 4, 5, and 9. So the class that formalizes the "relevant" part of the GDPR, called

`GDPR_Requirements`,

is defined as the intersection of the top-level requirements, unless data are not personal (in that case processing does not fall under the GDPR) or specific derogations apply as per Chapter 9. Accordingly, by means of an `EquivalentClasses` axiom, `GDPR_Requirements` is asserted to be equivalent to:

```
ObjectUnionOf(
   ObjectSomeValuesFrom(spl:hasData
     ObjectComplementOf(PersonalData)
   )
   ObjectIntersectionOf(
     Chap2_LawfulProcessing
     Chap3_RightsOfDataSubjects
     Chap4_ControllerAndProcessorObligations
     Chap5_DataTransfer
   )
   Chap9_Derogations
)
```
(1.3)

Informally speaking this means that, in order to be compliant with the GDPR, a business policy must either involve non-personal data only, or it should satisfy all the requirements encoded in the classes that formalize chapters 2–5, or it should be subject to the exceptions formalized by `Chap9_Derogations`.

Remark 1 (Alternative encoding approaches) In expression (1.3), the combination of `ObjectUnionOf` and `ObjectComplementOf` encodes the implication: "*if* data is personal, *then* chapters 2–5 or 9 must be fulfilled". While this is the exact encoding of the above implication, it falls outside SPECIAL's policy language $\mathcal{PL}$ (that does not support `ObjectComplementOf` because it makes compliance checking intractable). Since the above OWL2 expression is not in $\mathcal{PL}$, the explanation facility for (non) compliance decisions (cf. [1]) is not applicable. If a suitable explanation facility for the more general language is not available, then implications can be approximated in $\mathcal{PL}$ as follows:

```
ObjectUnionOf(
   ObjectSomeValuesFrom(spl:hasData
     NonPersonalData
   )
   ObjectIntersectionOf(
     Chap2_LawfulProcessing
     Chap3_RightsOfDataSubjects
     Chap4_ControllerAndProcessorObligations
     Chap5_DataTransfer
   )
   Chap9_Derogations
)
```
(1.4)

where NonPersonalData is a new class, that is asserted to be disjoint from the category of PersonalData with the axiom:

```
DisjointClasses( NonPersonalData PersonalData ).
```

This encoding *strengthens* the exact encoding, that is, the former implies the latter but not viceversa. As a consequence, the approximate encoding may erroneously notify that a policy is not compliant, while the opposite error – i.e. accepting a non-compliant policy – cannot happen. So the approximation is *safe*. Let us illustrate an example of how a policy may erroneously be considered non-compliant. Suppose that the category of BelgianEvents data is declared to be non-personal with the axiom:

```
DisjointClasses( BelgianEvents PersonalData ).
```
(1.5)

Now consider a policy that allows unrestricted processing of the data belonging to BelgianEvents, with no obligations and no legal basis:

```
ObjectIntersectionOf(
   ObjectSomeValueFrom( hasData BelgianEvents )
   ObjectSomeValueFrom( hasProcessing AnyProcessing )
   ObjectSomeValueFrom( hasPurpose AnyPurpose )
   ObjectSomeValueFrom( hasRecipient AnyRecipient )
   ObjectSomeValueFrom( hasStorage AnyStorage )
).
```

WIth the exact encoding (1.3), the above policy is correctly recognized to be compliant, because (1.5) implies:

```
SubClassOf(BelgianEvents ObjectComplementOf(PersonalData))
```

that is, Belgian events are not PersonalData (so they are not contrained by the GDPR, as formalized in (1.3)). However, (1.5) is too weak to conclude that the class of BelgianEvents is a subclass of NonPersonalData, that is, it is *not* possible to conclude that:

```
SubClassOf(BelgianEvents NonPersonalData).
```
(1.6)

Consequently, the conditions formulated by the approximate encoding (1.4) are not fulfilled: neither the data category in the above policy is `NonPersonalData`, nor the policy satisfies the requirements of chapters 2–5 or 9. The result is that the above policy is not a subclass of the approximate encoding (1.4), therefore it appears to be non-compliant when the approximate encoding is used. This kind of problems can be avoided by asserting that data are not personal with axiom (1.6), instead of (1.5). A similar, approximate encoding approach can be used also for the other occurrences of `ObjectComplementOf` used in the rest of this chapter. Hereafter, we illustrate the exact encodings and let the reader formulate the approximate version if needed. ∎

Now we proceed with the definition of the classes occurring in the exact encoding (1.3). The class `Chap2_LawfulProcessing` represents all the business policies that satisfy the articles in Chapter 2 of the GDPR with particular regard to legal bases (hence the name "lawful processing"). In turn, this class is defined in terms of classes that contain the policies that satisfy articles 6, 9, 10. In particular, each business policy should have a legal basis among those specified by Art. 6. In alternative, if the data involved in the processing are sensitive, then processing should be allowed by some of the legal bases in Art. 9. Finally, if criminal records are processed, then the additional restrictions of Art. 10 apply. This set of requirements is encoded in OWL2 by asserting that `Chap2_LawfulProcessing` is equivalent to:

```
ObjectUnionOf(
   Art6_LawfulProcessing
   Art9_SensitiveData
   Art10_CriminalData
)
```

In turn, `Art6_LawfulProcessing` is defined (with an `EquivalentClasses` axiom) as

```
ObjectUnionOf(
   ObjectSomeValuesFrom(spl:hasData
     ObjectComplementOf(PersonalData)[a]
   )
   ObjectSomeValuesFrom(spl:hasData
     SensitiveData_as_per_Art9
   )
   ObjectSomeValuesFrom(spl:hasData
     CriminalConvictionData_as_per_Art10
   )
   Art6_1_LegalBasis
   Art6_4_CompatiblePurpose
   )
)
```

[a] This complement operation is analogous to the one discussed in Remark 1.

that is, if data involved in the processing is personal but neither sensitive nor criminal conviction data, then the fundamental legal bases of Art. 6(1) apply, or the processing is compatible with the original purpose for collecting the data as per Art. 6(4).

In order to capture this meaning, class `Art6_1` is defined as:

```
ObjectSomeValuesFrom(hasLegalBasis
   ObjectUnionOf([a]
     Art6_1_a_Consent
     Art6_1_b_Contract
     Art6_1_c_LegalObligation
     Art6_1_d_VitalInterest
     Art6_1_e_PublicInterest
     Art6_1_f_LegitimateInterest
   )
)
```

[a] Although in $\mathcal{PL}$ unions are not explicitly allowed in the scope of properties, they are supported by SPECIAL's engine PLR through pre-processing.

Roughly speaking, this definition means that a business policy satisfies the requirements of Art. 6(1) if it contains a clause

`ObjectSomeValueFrom( hasLegalBasis` X `)`

where X is some of the above classes corresponding to points *a–f* of Art. 6(1).

Article 9 – when applicable (i.e. when data are classified as sensitive) – is dealt with by attaching to the business policy a legal basis corresponding to some of the points *a–j* of Art. 9(2). The definition of `Art9_SensitiveData` uses a new list of concepts to denote the new legal bases:

```
ObjectUnionOf(
   ObjectSomeValuesFrom(spl:hasData
     ObjectComplementOf(SensitiveData_as_per_Art9)
   )
   ObjectSomeValuesFrom(hasLegalBasis
     ObjectUnionOf(
       Art9_2_a_Consent
       Art9_2_b_EmploymentAndSocialSecurity
       Art9_2_c_VitalInterest
       Art9_2_d_LegitimateActivitiesOfAssociations
       Art9_2_e_PublicData
       Art9_2_f_Juducial
       Art9_2_g_PublicInteres
       Art9_2_h_PreventiveOrOccupationalMedicine
       Art9_2_i_PublicHealth
       Art9_2_j_ArchivingResearchStatistics
     )
   )
)
```

Informally speaking, this definition means that *if* a business policy concerns sensitive data[3] *then* it must contain a clause of the form

`ObjectSomeValueFrom( hasLegalBasis` X `)`

where X is some of the above classes corresponding to points *a–j* of Art. 9(2).

Article 10, instead adds some further constraints when the processing involves criminal records – in particular the controller must be suitably supervised. The corresponding concept `Art10_CriminalData` is defined as:

```
ObjectUnionOf(
   ObjectIntersectionOf(
     ObjectSomeValuesFrom(sbpl:hasDuty Art10_Requirements10)
     Refinements_as_per_Chap9
   )
   ObjectSomeValuesFrom(spl:hasData
     ObjectComplementOf(CriminalConvictionData_as_per_Art10)
   )
)
```

Informally speaking, the above definition says that either the processing does not involve criminal data, or the controller must satisfy the additional requirements laid out by Article 10 and, moreover, any further restrictions introduced by Chapter 9.

The class `Chap3_RightsOfDataSubjects` represents the obligation to support user rights introduced in Chapter 3 of the GDPR. The articles 12–22 of this chapter are collectively represented by a single class

`Art12-22_SubjectRights`

since either data are not personal (and those rights need not be supported), or the controller is obliged to support them all. Exceptions to this obligation are listed in Article 23. This set of requirements is encoded in OWL2 by asserting that the class `Chap3_RightsOfDataSubjects` is equivalent to:

```
ObjectUnionOf(
   Exceptions_as_per_Art23
   ObjectSomeValuesFrom(sbpl:hasDuty Art12-22_SubjectRights)
)
```

Roughly speaking, this definition says that either some exception listed in Article 23 restricts the user rights, or the controller must provide them all.

The class `Chap4_ControllerAndProcessorObligations` represents the obligations of the controller and the processor to implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR. The obligations introduced in Chapter 4 and in particular in Articles 32–37 are collectively represented by a single class

`Art32-37_Obligations`

[3] Cf. Remark 1.

since either data are not personal (and those obligations need not be implemented), or the controller and processor are obliged to implement them all. This set of requirements is encoded in OWL2 by asserting that `Chap4_ControllerAndProcessorObligations` is equivalent to:

```
ObjectSomeValuesFrom(sbpl:hasDuty Art32-37_Obligations)
```

The class `Chap5_DataTransferToThirdCountry` represents all the business policies that satisfy the articles in Chapter 5 of the GDPR with particular regard to transfer of personal data.

According to the GDPR, a transfer of personal data to a third country, i. e. a non-EU contry, may take place only if the third country ensures an adequate level of protection (cf. Article 45). However, if storage or recipients are located in a third country that does not occur in the list as per Article 45, then a transfer to a third country may take place only if the controller or processor has provided appropriate safeguards (cf. Article 46). Finally, if none of the previous articles applies, then transfer shall take place only on one of the derogations for a specific situation listed in Article 49. Consequently, `Chap5_DataTransferToThirdCountry` is asserted to be equivalent to:

```
ObjectUnionOf(
   ObjectIntersectionOf(
     Art48_TransfersNotAuthorisedByUnionLaw
     ObjectUnionOf(
       AdequateLevelOfProtection_as_per_Art45
       AppropriateSafeguards_as_per_Art46
       Art49_Derogations
     )
   )
   ObjectComplementOf(
     ObjectIntersectionOf(
       ObjectSomeValuesFrom(spl:hasProcessing svpr:Transfer)
       ObjectSomeValuesFrom(spl:hasStorage
         ObjectSomeValuesFrom(spl:hasLocation
              svl:ThirdCountries)
       )
     )
   )
)
```

In turn, `AppropriateSafeguards_as_per_Art46` is defined as a superclass of a set of classes formalizing the list of appropriate safeguards stated in Article 46, including binding corporate rules (cf. Article 47) as a special case:

```
Art46_2_a_PublicAuthorities
Art46_2_b_BindingCorporateRules_as_per_Art47
Art46_2_c_DataProtectionClausesAdoptedByEC
Art46_2_d_DataProtectionClausesAdoptedBySupervisoryAuthority
Art46_2_e_ApprovedCodeOfConduct
Art46_2_f_ApprovedCertificationMechanism
```

```
    Art46_3_a_ContractualClauses
    Art46_3_b_ProvisionsInAdministrativeArrangements
```

Informally speaking, this definition means that a business policy satisfies the requirements of Art. 46 if it contains a clause X where X is one of the above classes that represent points *a–f* of Art. 46(2) and points *a–b* of Art. 46(3).

Article 48, represented by the concept `Art48_TransfersNotAuthorisedBy UnionLaw` is defined as:

```
ObjectUnionOf(
   InternationalAgreement_as_in_Art48
   ObjectComplementOf(CourtRequestFromThirdCountry_as_in_Art48)
)
```

Article 49 - when applicable (i.e. in the absence of an adequacy decision pursuant to Article 45, and of appropriate safeguards pursuant to Article 46) - is dealth with by attaching to the business policy one of the exceptions for certain cases of international transfers corresponding to points *a–g* of Art. 49(1). The corrisponding concept `Art49_Derogations` is defined as:

```
ObjectIntersectionOf(
   ObjectUnionOf(
     Art49_1_a_Consent
     Art49_1_b_ContractByRequestOfDS
     Art49_1_c_ContractInInterestOfDS
     Art49_1_d_PublicInterest
     Art49_1_e_LegalClaims
     Art49_1_f_VitalInterest
     Art49_1_g_PublicData
   )
   ObjectComplementOf(AdequateLevelOfProtection_as_per_Art45)
   ObjectComplementOf(AppropriateSafeguards_as_per_Art46)
)
```

Informally speaking, this definition means that a business policy satisfies the requirements of Art. 49 if it contains a clause X where X is one of the above classes corresponding to points *a–g* of Art. 49(1).

As we already mentioned, the obligations and guidelines for the Union and Member States, and for the data protection authorities lie outside the scope of the formalization. Thus, Chapter 6, Chapter 7 and Chapter 8 will not be formalized.

Chapter 6 elaborates on the establishment of independent supervisory authorities responsible for monitoring and enforcing the application of the Regulation in each Member State. In particular, Art. 57 and Art. 58 state the tasks and powers - investigative, corrective, authorisation and advisory - of the Supervisory Authorities set out under the Regulation. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory

authorities shall cooperate with each other and the European Commission in accordance with Chapter 7.

Chapter 8 states further rights of data subjects. In particular, every data subject shall have *i.* the right to lodge a complaint with a supervisory authority and to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them; *ii.* the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation; and *iii.* the right to receive compensation from the controller or processor for a material or non-material damage suffered as a result of an infringement of this Regulation.

Chapter 9 has not been formalized, yet. It can be encoded in OWL2 by analogy with the other chapters, following the approach illustrated in this section.

Chapter 2

Formalizing the Pilot's Policies

The business policies illustrated in this chapter have been formulated based on the pilots defined by the industrial partners of SPECIAL, and verified by the legal experts of SPECIAL.

The starting point was an analysis of the business processes that implement the pilot; for each activity in each project, the pilot leader specified the data categories involved, the kind of processing, and all the other relevant properties of business policies. The purpose is typically determined by the application (e.g. event recommendations, compliance with financial regulations).

This chapter covers the policies for the pilots lead by Proximus and Thomson-Reuters. The policies for the pilot lead by DT are not included, since the final version of the pilot has been made available only recently.

2.1 Notation

When SPECIAL's framework is instantiated in a new application domain for the first time, it may be necessary to extend SPECIALs vocabularies by introducing subclasses of some of their terms (such as domain-specific data categories, purposes and processes, that are special cases of the general terms occurring in SPECIALs vocabularies). Such new term will be highlighted in bold.

In order to improve readability, hereafter on we will adopt a JSON-like syntax to express business policies. In patricular:

- { and } will be used do delimit compound concepts;
- + will indicate concept union;
- & and , will be used interchangeably to indicate concept intersection.

Finally, a role expression `ObjectSomeValuesFrom(R C)` will be abbreviated to {R: C}, where R is a role and C a concept expression.

2.2 Proximus

Proximus' pilot is an app for recommending events that take place on the Belgian coast, based on an interest profile that is inferred from the behavior of the user (such as internet navigation, phone calls, TV viewing choices).

Policy1: Ingest tourist events data for recommender system

This policy is associated to the process that imports from an external data source the data on the events that take place on the Belgian Coast. Since such data are not personal, this policy does not need to specify obligations and legal bases related to the GDPR. This is the only policy that does not involve any personal data.

```
{
  {spl:hasData:  NonPersonalData},
  {spl:hasProcessing:  svpr:IncomingTransfer},
  {spl:hasPurpose:  RecommendBelgianCoastEvents},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {
      {spl:hasDuration:  svd:BusinessPractice},
      {spl:hasLocation:  svl:EU & svl:ProcessorServers}
    }
  }
}
```

Policy2: Ingest Proximus service usage data for recommender system

This policy describes the collection of data about the user, including behavioral data. The latter is generated by the user's internet navigation activity, phone calls, and TV choices. The legal basis in this case is consent.

```
{
  {spl:hasData:  PersonalData &
    {
     svd:AudiovisualActivity + svd:Demographic + svd:Location +
     svd:Navigation + svd:OnlineActivity + svd:TelecomActivity
    }
  },
  {spl:hasProcessing:  svpr:Collect + svpr:Tracking} ,
  {spl:hasPurpose:  RecommendBelgianCoastEvents},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasDuration:  svd:StatedPurpose},
    {spl:hasLocation:  svl:EU & svl:ProcessorServers},
    {spl:durationInDays:  [0,42]}
  },
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations},
  {hasLegalBasis:  Art6_1_a_Consent}
}
```

Policy3: Collect personal information for contacting the data subject

This policy is needed for the collection of demographic and contact data when the contract with the customer is signed. Such information is used for contacting the customer for contractual purposes (like billing and notifications). The legal base, in this case, is the performance of a contract.

```
{
  {spl:hasData:  PersonalData &
    {svd:Demographic + svd:Online + svd:Physical}
  },
  {spl:hasProcessing:  svpr:Collect},
  {spl:hasPurpose:  svpu:AnyContact},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasDuration:  svd:BusinessPractice},
    {spl:hasLocation:  svl:EU & svl:ControllerServers}
  },
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations},
  {hasLegalBasis:  Art6_1_b_Contract}
}
```

Policy4: Collect or update personal interest of the data subject

This policy is associated to the interface through which customers may directly modify their own personal data and the interest profile created by the recommendation system. This process updates the aforementioned data on behalf of the user, based on the consent initially granted by the customer when the recommendation app is installed.

```
{
  {spl:hasData:  PersonalData & Profile4RecommenderSystem},
  {spl:hasProcessing:  svpr:Update},
  {spl:hasPurpose:  RecommendBelgianCoastEvents},
  {spl:hasRecipient:  svr:Ours}
  {spl:hasStorage:
    {spl:hasDuration:  svd:BusinessPractice},
    {spl:hasLocation:  svl:EU & svl:ControllerServers}   },
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations},
  {hasLegalBasis:  Art6_1_a_Consent}
}
```

Policy5: Create a personal interest profile for a data subject

This policy is associated to the process that classifies customers based on their behavioral data, creating the profile mentioned in the previous policy. The legal basis is the consent given when the recommendation app is installed.

```
{
  {spl:hasData:  PersonalData &
    {
     svd:AudiovisualActivity + svd:Location + svd:Navigation +
     svd:OnlineActivity + svd:Preference + svd:TelecomActivity
    }
  },
  {spl:hasProcessing:  svpr:Analyse},
  {spl:hasPurpose:  RecommendBelgianCoastEvents},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasDuration:  svd:StatedPurpose},
    {spl:hasLocation:  svl:EU & svl:ProcessorServers},
    {spl:durationInDays:  [0,42]}
  },
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations},
  {hasLegalBasis:  Art6_1_a_Consent}
}
```

Policy6: Link an event to a data subject's personal interest

This is the policy associated to the actual recommendation activity. The information about the customer is used to select the events that may be of interest for her.

Assumption: Demographic is not part of the Profile4RecommenderSystem.

```
{
  {spl:hasData PersonalData &
    {Profile4RecommenderSystem + svd:Demographic + svd:Location}
  },
  {spl:hasProcessing:
     svpr:Aggregate + svpr:Analyse + svpr:Query
  },
  {spl:hasPurpose:  RecommendBelgianCoastEvents},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasDuration:  svd:BusinessPractice},
    {spl:hasLocation:  svl:EU & svl:ControllerServers}
  },
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations},
  {hasLegalBasis:  Art6_1_a_Consent}
}
```

2.3 Thomson Reuters

This pilot is about complying with financial regulations. They require to create risk profiles for financial transactions, based on information about the involved entities, including the persons that play a crucial role (such as CEOs and owners). Such risk profiles are then shared with TR's customers.

Policy1: Take documentary evidence of identity and generate identity information

This policy is associated to the collection of personal information. Such information may consist of paper documents, possibly including passports. The legal basis is consent.

```
{
  {spl:hasData:  PersonalData &
    { svd:Demographic + svd:Financial + svd:Government}
  },
  {spl:hasProcessing:
     svpr:Aggregate + svpr:Archive + svpr:Copy
  },
  {spl:hasPurpose:  ComplianceWithFinancialRegulation},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasLocation:  UK & svl:ControllerServers},
    {spl:durationInDays:  [0, 1826]}
  },
  {hasLegalBasis:  Art6_1_a_Consent},
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations}
}
```

Policy2: Store identity information

This policy applies to the subsequent organization of collected information and its persistent preservation, which includes the creation of internal identifiers for the persons involved.

```
{
  {spl:hasData:  PersonalData &
    { svd:Demographic + svd:Physical + svd:Social }
  },
  {spl:hasProcessing:  svpr:Archive + svpr:ApplyIdentifier},
  {spl:hasPurpose:  ComplianceWithFinancialRegulation},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasLocation:  UK & svl:ControllerServers},
    {spl:durationInDays:  [0, 1826]}
  },
  {hasLegalBasis:  Art6_1_a_Consent},
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations}
}
```

Policy3: Screen identity infomation

This policy describes the subsequent queries to personal information, that are carried out during the construction of risk profiles.

```
{
  {spl:hasData:  PersonalData &
     {svd:Demographic + svd:Physical + svd:Social }
  },
  {spl:hasProcessing:  Query},
  {spl:hasPurpose:  ComplianceWithFinancialRegulation},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasLocation:  UK & svl:ControllerServers},
    {isHeld:  InMemory},
    {durationOf:  Query},
    {spl:durationInMinutes:  [0, 5]}
  },
  {hasLegalBasis:  Art6_1_a_Consent},
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations}
}
```

Policy4: Make risk assesment

This policy describes the collection of public information about the persons of interest. This information is archived and manually analyzed to build a risk profile.

```
{
  {spl:hasData:  PersonalData &
    {AdverseInformation + NegativeMedia}
  },
  {spl:hasProcessing:  svpr:Archive + svpr:Derive},
  {spl:hasPurpose:  ComplianceWithFinancialRegulation},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasLocation:  UK & svl:ControllerServers},
    {spl:durationInDays:  [0, 1826]}
  },
  {hasLegalBasis:  Art6_1_a_Consent},
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations}
}
```

Policy5: Save identity profile and risk assesment

The information about the person of interest and the related risk profile are stored within TR's systems. TR's customers (which are formalized with OtherRecipient, that is the term that denotes third parties) may access this information. Also this operation requires the consent of the data subject.

```
{
  {spl:hasData:  PersonalData &
    {IdentityProfile + RiskProfile}
  },
  {spl:hasProcessing:  svpr:Archive},
  {spl:hasPurpose:  ComplianceWithFinancialRegulation},
  {spl:hasRecipient:  svr:OtherRecipient},
  {spl:hasStorage:
    {spl:hasLocation:  UK & svl:ControllerServers},
    {spl:durationInDays:  [0, 1826]}
  },
  {hasLegalBasis:  Art6_1_a_Consent},
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations}
}
```

Policy6: Share identity profile and risk assesment

Finally, the information about the person of interest and the related risk profile can be transferred to TR's customers. This policy is similar to the previous one.

```
{
  {spl:hasData:  PersonalData &
    {IdentityProfile + RiskProfile}
  },
  {spl:hasProcessing:  svpr:OutgoingTransfer},
  {spl:hasPurpose:  ComplianceWithFinancialRegulation},
  {spl:hasRecipient:  svr:OtherRecipient},
  {spl:hasStorage:
    {spl:hasLocation:  UK & svl:ControllerServers},
    {spl:durationInDays:  [0, 1826]}
  },
  {hasLegalBasis:  Art6_1_a_Consent},
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations}
}
```

Chapter 3

Compliance with GDPR's formalization

In this chapter, we illustrate the automated validation of business policies, based on the formalization of the GDPR described in Chapter 1. The examples reported here are taken from the validation tests that we carried out on the formalization and on pilot policies.

The automated compliance tests w.r.t. the formalization of the GDPR make it is possible to verify that the different properties of the given business policy are coherent with each other, thereby preventing some possible human errors. For example,

- if data are personally identifiable, then the policy must contain the duties associated to data subjects rights, such as those in Art. 12–22 and Art. 33–34;
- if data are sensitive, then the legal basis should be based on Art. 9;
- if data involve criminal records, then the requirements of Art. 10 should be fulfilled;
- if storage or recipients are located in a third country that does not occur in the list as per Art. 45, and the recipient is an organization that does not occur in that same list, then ordinary consent does not suffice and additional requirements apply, see for example Art. 46 or Art. 49 of the GDPR.

All the business policy reported in Section 2.2 and Section 2.3 are compliant with the Regulation. In order to show that all the components of the business policies are essential in order to comply to the GDPR formalization, consider eliminating the last conjunct of the Proximus' second business policy:

```
{
  {spl:hasData:  PersonalData &
    {
     svd:AudiovisualActivity + svd:Demographic + svd:Location +
     svd:Navigation + svd:OnlineActivity + svd:TelecomActivity
    }
  },
  {spl:hasProcessing:  svpr:Tracking} ,
  {spl:hasPurpose:  RecommendBelgianCoastEvents},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasDuration:  svd:StatedPurpose},
    {spl:hasLocation:  svl:EU & svl:ProcessorServers},
    {spl:durationInDays:  [0,42]}
  },
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations},
}
```

Policy2_a_Proximus

Then compliance fails. The diagnostic engine notifies the authors that compliance needs to be supported by one of the legal basis specified by Art. 6.

We obtain other examples of non compliant business policies by eliminating the penultimate (resp. antepenult) conjunct of Proximus' second business policy which result in Policy2_b_Proximus (resp. Policy2_c_Proximus) below.

```
{
  {spl:hasData:  PersonalData &
    {
     svd:AudiovisualActivity + svd:Demographic + svd:Location +
     svd:Navigation + svd:OnlineActivity + svd:TelecomActivity
    }
  },
  {spl:hasProcessing:  svpr:Tracking} ,
  {spl:hasPurpose:  RecommendBelgianCoastEvents},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasDuration:  svd:StatedPurpose},
    {spl:hasLocation:  svl:EU & svl:ProcessorServers},
    {spl:durationInDays:  [0,42]}
  },
  {sbpl:hasDuty:  Art32-37_Obligations},
  {hasLegalBasis:  Art6_1_a_Consent}
}
```

Policy2_b_Proximus

```
{
  {spl:hasData:  PersonalData &
    {
     svd:AudiovisualActivity + svd:Demographic + svd:Location +
     svd:Navigation + svd:OnlineActivity + svd:TelecomActivity
    }
  },
  {spl:hasProcessing:  svpr:Tracking} ,
  {spl:hasPurpose:  RecommendBelgianCoastEvents},
  {spl:hasRecipient:  svr:Ours},
  {spl:hasStorage:
    {spl:hasDuration:  svd:StatedPurpose},
    {spl:hasLocation:  svl:EU & svl:ProcessorServers},
    {spl:durationInDays:  [0,42]}
  },
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {hasLegalBasis:  Art6_1_a_Consent}
}
```

Policy2_c_Proximus

Then the diagnostic engine notifies the authors that a required duty is not reported in the policy, namely, the support of user rights as per Chapter 3 (resp. the notification, protection, and risk assessment obligations required by Chapter 4) of the GDPR.

Another group of non compliant business policies can be obtained considering the requirements formalized in `Chap5_DataTransferToThirdCountry`. Suppose we modify the storage location of Thomson Reuters' Policy 6 in order to say that the outgoing data transfer is carried out towards a third country. As a consequence Chapter 5 of the Regulation come into play, thus resulting in a non complient business policy:

```
{
  {spl:hasData:  PersonalData &
    {IdentityProfile + RiskProfile}
  },
  {spl:hasProcessing:  svpr:OutgoingTransfer},
  {spl:hasPurpose:  ComplianceWithFinancialRegulation},
  {spl:hasRecipient:  svr:OtherRecipient},
  {spl:hasStorage:
    {spl:hasLocation:  svl:ThirdCountries},
    {spl:durationInDays:  [0, 1826]}
  },
  {hasLegalBasis:  Art6_1_a_Consent},
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations}
}
```

Policy6_TR_a

To meet the requirements posed by the Regulation, the business policy must specify which conditions (among `AdequateLevelOfProtection_as_per_Art45`, `AppropriateSafeguards_as_per_Art46` or `Art49_Derogations`) laid down in Chapter 5 are complied with by the controller and processor. Note, however, that according to `Chap5_DataTransfer`, the business policy should explicitly state compliance with the conditions of Art. 48 – therefore the business policy Policy6_TR_b is still not compliant with the Regulation, while the Policy6_TR_c is. Recall that the opposite case, i.e. the transfer or disclosure of personal data based on an international agreement between the requesting third country and the Union or a Member State, would imply that the destination country qualifies as `spl:EULike` and not `spl:ThirdCountry` in the terminology adopted in D2.5. That is, the destination country should be in a list of countries approved by the EU.

```
{
  {spl:hasData:  PersonalData &
    {IdentityProfile + RiskProfile}
  },
  {spl:hasProcessing:  svpr:OutgoingTransfer},
  {spl:hasPurpose:  ComplianceWithFinancialRegulation},
  {spl:hasRecipient:  svr:OtherRecipient},
  {spl:hasStorage:
    {spl:hasLocation:  svl:ThirdCountries},
    {spl:durationInDays:  [0, 1826]}
  },
  AdequateLevelOfProtection_as_per_Art45,
  {hasLegalBasis:  Art6_1_a_Consent},
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations}
}
```

Policy6_TR_b

```
{
  {spl:hasData:  PersonalData &
    {IdentityProfile + RiskProfile}
  },
  {spl:hasProcessing:  svpr:OutgoingTransfer},
  {spl:hasPurpose:  ComplianceWithFinancialRegulation},
  {spl:hasRecipient:  svr:OtherRecipient},
  {spl:hasStorage:
    {spl:hasLocation:  svl:ThirdCountries},
    {spl:durationInDays:  [0, 1826]}
  },
  AdequateLevelOfProtection_as_per_Art45,
  Art48_TransfersNotAuthorisedByUnionLaw,
  {hasLegalBasis:  Art6_1_a_Consent},
  {sbpl:hasDuty:  Art12-22_SubjectRights},
  {sbpl:hasDuty:  Art32-37_Obligations}
}
```

Policy6_TR_c

Bibliography

[1] P.A. Bonatti, L. Ioffredo, S. Mosi, I.M. Petrova, and L. Sauro. Advanced queries and explanations. Technical Report WP4-CeRICT-1, SPECIAL, Dec. 2019.