ONTOROPA
D2. 'PROPOSED DESIGN SPECIFICATION AND APPROACH'

24/05/2021

Grant Agreement No.: 957338
Call: H2020-ICT-2020-1

Topic: ICT-54-2020
Type of action: RIA

ONTOROPA

D2. 'PROPOSED DESIGN SPECIFICATION AND APPROACH'

DUE DATE	24/05/2021
SUBMISSION DATE	24/05/2021
TEAM	ONTOROPA
VERSION	1.0
AUTHORS	M.Mercedes Martínez-González, Pompeu Casanovas, María-Luisa Alvite-Díez, Núria Casellas, Inma Gutiérrez
COLLABORATORS	María Ruíz, David Sanz, Amador Aparicio, Sergio Miguel

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

EXECUTIVE SUMMARY

OntoROPA deals with the automated creation and maintenance of a critical piece of legal compliance required by the GDPR—the *Records of Processing Activities* (ROPA). It includes the design of a knowledge graph—an RDF graph—to handle information about ROPAs, combining a legal professional ontology (which will be a part of this graph) with the collection and management of the specific knowledge of the community of privacy and data protection experts.

The OntoROPA architecture is law and data driven. ROPAs are deemed to be the critical piece of legal compliance from a social perspective: they are the only available source of information, accessible to non-technical people (including citizens, judges, rulers, law experts, data protection users, and supervisors). Thus, this fact makes them a critical piece for GDPR legal compliance for all stakeholders—providers, controllers, supervisors, and companies. This is a market niche.

Deliverable 2, *OntoROPA proposed design specification and approach*, is focused on a modular, distributed, and ontological approach for the design of both layers—software and data—*where each module is the answer to a legal requirement.* Data comply with standards for the aim of interoperability, and the design of both layers are subjected to a legal governance scheme, specifically set to harmonize an innovative design for the marketplace with the law, policy, and ethics framework. On top of that, Deliverable 2 explores the possibilities that blockchain technology offers: the use of TEE for secure processing, the use of verifiable credentials with standard certificates for identity management, and the use of oracles for accessing external services.

In Deliverable 2, **Section 1** introduces the main contents.
Section 2 presents a solution with two main components: (1) An OWL ontology that collects the expert knowledge from the target domain (ROPA community) for supporting validation and trustworthiness; (2) and the software artifacts that process ROPAs. This section (i) introduces OntoROPA modules—identity, linked RDF ROPAs, validation, certification, proactiveness—,(ii) offers a detailed design specification (ontology and software requirements, methodology, OntoROPA flowchart) (iii) and describes the interfaces for coordination with ONTOCHAIN blocks.
Section 3 deals with the impacts. It includes the business model to get into the market as a new Law-Tech Web Service. It describes its main features, the OntoROPA contribution to bridging web semantics and blockchain technologies, and it defines the creation of ONTOCHAIN legal value. *Legal knowledge* (legal justification) is also required by the Spanish legislation for ROPAs. OntoROPA legal governance system, the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

middle-out and *inside-out* approaches aligned with EU strategies and policies, and the generation of the OntoROPA regulatory legal ecosystem, are explained in detail, including the compatibility between blockchain solutions and GDPR requirements.
Section 4 copes with the implementation process, comprising ontology modularity, software modularity, and real time performance of the solution (Ontology and Software KPIs, experimental evaluation, and interoperability aspects, followed by a granular implementation plan). This is heading to an *OntoROPA standardisation process*. Finally, **Section 5**, highlights in the Conclusion some results and what is next.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

TABLE OF CONTENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

LIST OF FIGURES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

LIST OF TABLES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

ABBREVIATIONS

GDPR	General Data Protection Regulation
ROPA	Records Of (Personal) Data Processing Activities
LOPD	Ley orgánica de Protección de Datos
KPIs	Key Performance Indicators
TEE	Trusted Executed Environment
LDAP	Lightweight Directory Access Protocol
MiCA	European Commission´s Regulation of Markets in Crypto-assets

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

1 INTRODUCTION

OntoROPA implements smart privacy legal compliance using technologies capable of providing semantics, intelligence, and trust. OntoROPA focuses on the creation and maintenance of a critical piece of legal compliance required by the GDPR (Regulation EU 2016/679), the Records of Processing Activities (ROPA).[1]

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

These records are an instrument of legal compliance for private and public individuals and organizations that manage personal data. They provide an inventory of the data processing activitites performed on private data and maintaining such records is an obligation for controllers and processors.

> *1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.*

ROPAs have to contain a specific amount of information and they have to be kept in electronic form.

> *3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.*

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e3033-1-1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Currently, most of these records are created manually and mantained in word documents or excel files and made available to the public mostly in their original formats or as pdfs.

TRATAMIENTO	CONSEJERÍA	CENTRO DIRECTIVO	RESPONSABLE DEL TRATAMIENTO	DELEGADO DE PROTECCIÓN DE DATOS	BASE JURÍDICA	FINES DEL TRATAMIENTO
Registro base de datos de licitadores y contratistas de la Plataforma electrónica Duero de la Junta de Castilla y León	Consejería de Economía y Hacienda	Secretaría General	Secretaría General C/ José Cantalapiedra,2.47014 Valladolid. Teléfono 983 414000. Correo electrónico duero.funcionales@jcyl.es	Consejería de Economía y Hacienda C/ José Cantalapiedra,2. 47014 Valladolid. Teléfono 983 4140000. Correo electrónico: dpd.economiayhacienda@jcyl.es	Artículo 6.1.c) del RGPD, tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento y 6.1e) del RGPD, es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. Ley 9/2017 de 8 de noviembre, de Contratos del Sector público	Tramitar electrónicamente los procedimientos de contratación en todas sus fases y posibiltar las relaciones y comunicaciones con licitadores y contratistas. Los datos personales podrán ser tratados para fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos de acuerdo con lo establecido en los artículos 5.1 b) y 89.1 del RGPD.
Registro de Colegios Profesionales y Consejos de Colegios de Castilla y León	Consejería de Economía y Hacienda	Secretaría General	Secretaría General C/ José Cantalapiedra,2.47014 Valladolid. Teléfono 983 414000. Correo electrónico sgeconomiayhacienda@jcyl.es	Consejería de Economía y Hacienda.C/ José Cantalapiedra,2.47014 valladolid.Teléfono 983 414000. Correo electrónico dpd.economiayhacienda@jcyl.es	Artículo 6.1c) del RGPD , es necesario para el cumplimiento de una obligación legal. Ley 8/1997, de 8 de julio, de Colegios Profesionales de Castilla y León.	Dar publicidad registral a los actos relativos a colegios Profesionales y Consejos de Colegios de acuerdo con la normativa. Los datos personales podrán ser tratados para fines de archivo en interés público, de investigación científica e histórica o fines estadísticos de acuerdo artículos5.1b) y 89.1 del RGPD
Gestión de recursos humanos de la Consejería de Economía y Hacienda de la Junta de Castilla y león.	Consejería de Economía y Hacienda	Secretaría General.	Secretaría General C/ José Cantalapidra,2.47014 Valladolid. Teléfono 983 414000. Correo electrónico sgeconomiayhacienda@jcyl.es	Consejería de Economía y Hacienda.C/ José Cantalapiedra,2.47014 Valladolid.Teléfono 983 414000. Correo electrónico dpd.economiayhacienda@jcyl.es	Artículo 6.1e) del RGPD, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.Ley 7/2005, de 24 de mayo, de la Función Pública de Castilla y León. Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los	Gestión de los recursos humanos de la Consejería de Economía y Hacienda de la Junta de Castilla y León. Los datos personales podrán ser tratados para fines de archivo en interés público, de investigación científica e histórica o fines estadísticos de acuerdo artículos5.1b) y 89.1 del RGPD.
Procesos de selección de personal temporal de la Consejería de Economía y Hacienda.	Consejería de Economía y Hacienda	Secretaría General	Secretaría General C/ José Cantalapiedra,2.47014 Valladolid. Teléfono 983 414000. Correo electrónico sgeconomiayhacienda@jcyl.es	Consejería de Economía y Hacienda.C/ José Cantalapiedra,2.47014 Valladolid.Teléfono 983 414000. Correo electrónico dpd.economiayhacienda@jcyl.es	Artículo 6. 1e) , cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos y 6.1c) del RGPD para el cumplimiento de una obligación legal. Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.Ley 7/2005, de 24 de mayo, de la Función Pública de Castilla y León. Real Decreto Legislativo 2/2013, de 23 de octubre, por el que se aprueba el texto	Procesos de selección de personal interinoy/o laboral eventual para su incorporación a la Consejería de Economía y Hacienda. Los datos personales podrán ser tratados para fines de archivo en interés público, de investigación científica e histórica o fines estadísticos de acuerdo artículos5.1b) y 89.1 del RGPD
Controles de acceso y videovigilancia de la Consejería de Economía y Hacienda	Consejería de Economía y Hacienda	Secretaría General	Secretaría General C/ José Cantalapidra,2.47014 Valladolid. Teléfono 983 414000. Correo electrónico sgeconomiayhacienda@jcyl.es	Consejería de Economía y Hacienda.C/ José Cantalapiedra,2.47014 valladolid.Teléfono 983 414000. Correo electrónico dpd.economiayhacienda@jcyl.es	Artículo 6.1e) RGPD, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos .Ley 5/2014, de 4 de abril, sde Seguridad Privada. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.	Garantizar la seguridad de personas, bienes e instalaciones, así como el registro y control de acceso de las personas en los edificios de la Consejería Economía y Hacienda.
Registro de altos cargos como miembros de Consejos de Administración en empresas publicas y participadas o de Organos colegiados de Organismos Publicos	Consejería de Economía y Hacienda	Secretaría General.	Secretaría General C/ José Cantalapiedra,2.47014 Valladolid. Teléfono 983 414000. Correo electrónico sgeconomiayhacienda@jcyl.es	Consejería de Economía y Hacienda.C/ José Cantalapiedra,2.47014 Valladolid.Teléfono 983 414000. Correo electrónico dpd.economiayhacienda@jcyl.es	Artículo 6.1e) RGPD, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos . Ley 3/2016, de 30 de noviembre, del Estatuto de los Altos Cargos de la Administración de la Comunidad de Castilla y León	Inscripción de los altos cargos que sean miembros de los Consejos de Administración en empresas públicas y participadas de la Comunidad, o de órganos colegiados de organismos públicos. Los datos personales podrán ser tratados para fines de archivo en interés público, de investigación científica e histórica o fines estadísticos de acuerdo artículos5.1b) y 89.1 del RGPD
Procedimiento sancionador en Defensa de la Competencia.	Consejería de Economía y Hacienda	Secretaría General.	Secretaría General C/ José Cantalapiedra,2.47014 Valladolid. Teléfono 983 414913. Correo electrónico defensa.competencia@jcyl.es	Consejería de Economía y Hacienda.C/ José Cantalapiedra,2.47014 Valladolid.Teléfono 983 414000. Correo electrónico dpd.economiayhacienda@jcyl.es	Artículo 6.1e) RGPD, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos . Ley 15/2007, de 3 de julio, de Defensa de la Competencia.	Tramitación de los expedientes sancionadores en materia defensa competencia. Denuncias e instrucción de expedientes, recogida de datos de las partes intervinientes y de cualquier tercero con relevancia. Los datos personales podrán ser tratados para fines de archivo en interés público, de investigación científica e histórica o fines estadísticos de acuerdo artículos5.1b) y 89.1 del RGPD
Promoción en Defensa de la Competencia.	Consejería de Economía y Hacienda.	Secretaría General .	Secretaría General C/ José Cantalapidra,2.47014 Valladolid. Teléfono 983 414913. Correo electrónico defensa.competencia@jcyl.es	Consejería de Economía y Hacienda.C/ José Cantalapiedra,2.47014 valladolid.Teléfono 983 414000. Correo electrónico dpd.economiayhacienda@jcyl.es	Artículo 6.1e) RGPD, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos . Ley 15/2007, de 3 de julio, de Defensa de la Competencia.	Actos de promoción de la competencia dirigidos a prevenir la vulneración de la normativa en esta materia. Los datos personales podrán ser tratados para fines de archivo en interés público, de investigación científica e histórica o fines estadísticos de acuerdo artículos5.1b) y 89.1 del RGPD

Figure 1.Example of a publicly available ROPA from a public administration (Spain).

OntoROPA thus aims at the creation of a ROPA knowledge graph that will include not only the legal requirements but also the practical knowledge from the community of privacy and data protection experts—mainly including lawyers, legal advisors and scholars, data protection officers, and rulers who are proficient in the creation and manipulation of ROPAs.

The notion of practical knowledge is crucial because this entails an implicit professional knowledge that must be elicited and make explicit in the knowledge acquisition process.

This kind of knowledge will be also modelled, as it encompasses the professional selection and understanding of legal normative texts and provisions, and it is not to be found in legal documents containing positive law—it belongs to the experience of lawyers, especially controllers and supervisors.

This includes the interpretation of hard law, soft law, policies and ethics (as it will be explained later).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

2 DESIGN SPECIFICATION AND APPROACH

2.1 SOLUTION DESCRIPTION, ARCHITECTURE DIAGRAM AND USE CASE SCENARIO

2.1.1 Description

Our solution has two main components:

1) An OWL ontology that collects the expert knowledge from the target domain (ROPA community) and is the tool directing the inference processes that support validation and trustworthiness.

2) The software artifacts that process ROPAs.

In this document, we focus on the scenario and use case that will be solved during First Call. The target community of users are ROPA providers (ROPA controllers). The OntoROPA ecosystem will support more communities of ROPA users. For example, data protection supervisors are able to assess ROPAs. However, citizens are not able to assess ROPAs, but to read and query the information that ROPAs can provide to them about the way their personal data are treated, and protected. A general solution, able to support different communities, requires a long-term project. For further information about this, please, refer to section 4. Implementation.

The final solution entails the creation of a Law Tech legal web service to provide automated ROPAs to law firms, companies and administrations. This also entails the definition of a business model that fits into the niche of Data Protection and Privacy Services, as advanced by the European Digital Markets strategy. We will provide a preliminary hint of it in Section 3.

Ontology Description

OntoROPA proposes the development of a domain ontology formally expressed in OWL that will be offered as open data, reliable, reusable, and extensible. This professional ontology will support the creation and validation of ROPAs. Validation will be twofold: RDF validation for correctness and OWL validation for completeness.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

The ROPA Ontology will not only include legal but also professional knowledge extracted from the community of privacy and data protection experts—mainly including lawyers, legal advisors and scholars, data protection officers, and rulers who are proficient in the creation and manipulation of ROPAs.

As a preliminary proof of concept of the ROPA Ontology, we present the following ROPA RDF description, which can be validated for correctness and a preliminary ontology sample that demonstrates the reasoning capabilities for completeness of legal-compliance standard validation.

```
@prefix ropa: <http://www.ontoropa.org/ropa#> .
@prefix skos: <http://www.w3.org/2004/02/skos/core#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .

<http://www.ontoropa.org/ropa-data#c4cc78ad-a91a-4ba2-a16d-cb1071e513c4>
  a <http://www.ontoropa.org/ropa#RecordOfProcessingActivity> ;
  ropa:hasController <http://www.ontoropa.org/ropa-data#1f949248-18ae-4fd5-be21-
38ac2e364843> ;
  ropa:hasRepresentative <http://www.ontoropa.org/ropa-data#735922d1-5f53-4dda-8aac-
0e1df7b69bbb> ;
  ropa:hasProcessingPurpose <http://www.ontoropa.org/ropa-voc/processing-
purposes#purpose13> ;
  ropa:hasDataSubjectCategory <http://www.ontoropa.org/ropa-voc/data-subject-
categories#subject-category22> ;
  ropa:hasPersonalDataCategory <http://www.ontoropa.org/ropa-voc/personal-data-
categories#data-category4> .

<http://www.ontoropa.org/ropa-voc/processing-purposes#purpose13>
  a ropa:ProcessingPurpose ;
  skos:prefLabel "Tramitación de ayudas y subvenciones"@es ;
  skos:definition "Tramitación de las ayudas y subvenciones gestionadas por la Dirección
General de Competitividad de la Industria Agroalimentaria y de la Empresa Agraria."@es .

<http://www.ontoropa.org/ropa-voc/data-subject-categories#subject-category22>
  a ropa:DataSubjectCategory ;
  skos:prefLabel "Personas físicas"@es ;
  skos:definition "Personas físicas, así como aquellas personas físicas que representen a las
personas jurídicas, que tengan la condición de interesadas en las diferentes subvenciones y
ayudas, que se gestionan por la Dirección General."@es .

<http://www.ontoropa.org/ropa-voc/personal-data-categories#data-category4>
  a ropa:PersonalDataCategory ;
  skos:prefLabel "Nombre"@es ;
  skos:altLabel "Datos de identificación de las personas físicas: Nombre"@es .

ropa:PersonalDataCategory rdfs:subclassOf skos:Concept .
ropa:DataSubjectCategory rdfs:subclassOf skos:Concept .
ropa:ProcessingPurpose rdfs:subclassOf skos:Concept .
```

Figure 2. Ropa RDF Description

First, the RDF can be validated for its syntax correctness[2]
Then, the entity can be validated for completeness against the ontology

[2] https://www.w3.org/RDF/Validator/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

model for ROPA using Pellet (verification against the axiom restrictions for the ROPA class).

2.1.2 Architecture diagram

OntoROPA uses a modular approach, where each module serves a specific functionality. This modular approach will facilitate OntoROPA **resilience to changes in collaborators**.

For example, we can either take in charge the Identity module with the development of **our own oracle**, able to validate X509[3] digital certificates in LDAP services or to use services provided by HIBI and/or SSiVault (see section 2.4 for interactions with the other Ontochain blocks).

Moreover, it will guide the implementation steps presented in the implementation plan of section 4.4. Figure 3 shows the main modules in OntoROPA software ecosystem.

A very important component of OntoROPA are **data**: ROPAs, ontologies, and data that helps to achieve the desired facilities, such as certificates and credentials used for identity verification. Figure 4 includes the data layer with modules in Figure 3. These data are critical for OntoROPA modules: they are inputs and outputs. More important, they determine the design of each module. This is a data-driven design.

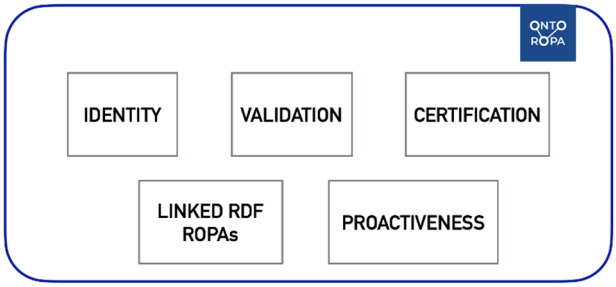

Figure 3. Main OntoROPA modules.

[3] (X.509 certificates are digital certificates that use the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the hostname/domain, organization, or individual contained within the certificate)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

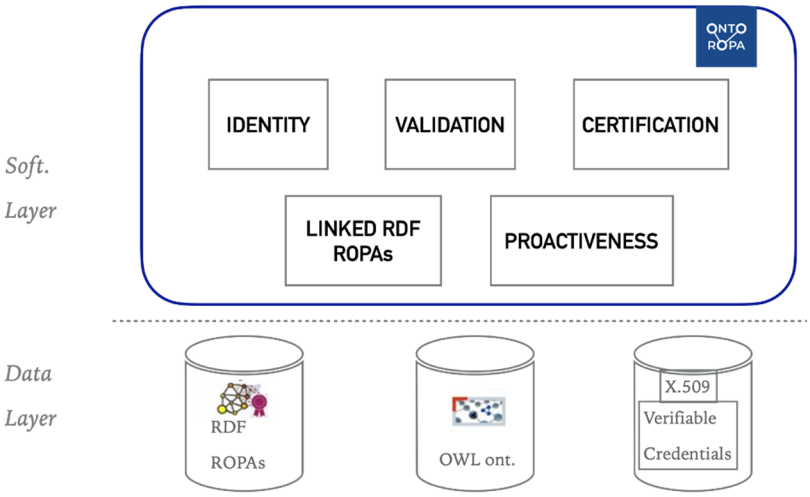

Figure 4. Main OntoROPA modules and data.

The OntoROPA modules are:

- **IDENTITY:**
  Legal compliance requires being able to link responsibilities and authorhisp to legal entities, real world entities. X.509 certificates will be used. Verification of these certificates requires to query LDAP directories. This task can be in charge of services provided by other ONTOCHAIN projects, HIBI and/or OntoSSiVault. If this is not possible an ad-hoc oracle would be needed.

- **LINKED RDF ROPAs:**
  The OntoROPA project aims to represent ROPA as RDF graphs, linked with the ONtoROPA ontology, but also to other ROPAs. RDF, linked data and related Semantic Web standards provide the tools to represent, share and manage semantics in technical environments. Storage will rely on the facilities provided by GraphChain, a solution able to store and manage RDF graphs on blockchain. If not possible, an external RDF store, e.g. AllegroGraph, may be needed.

- **VALIDATION:** ROPAs should comply with article 30 of the GDPR[2] and with the *non-written rules of use* that the community of experts, ROPA controllers, follow when creating them. This knowledge will be collected in the OntoROPA ontology. The validation will be done against the ontology, using the inference capabilities associated to OWL rules and inference. We would like this validation to be a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

secure process, not subject to injections. However, as we do not know of any project that offers such facilities in Ontochain, we may need to use external services for this aim, for example, WebProtégé. In such a case, the interactions with the blockchain will limit to the results of validation. The proof of validation will be taken in charge off-chain by OntoROPA, with its own signature and certificates.

- **CERTIFICATION:** ROPAs origin and provenance should be certified. As well, the results of processes such as validation should be certified by OntoROPA. For ROPA provenance, GraphChain provides support. As for the results of validation, it depends on the viability of secure executions, as we stated in previous item. If the process can be secured in a blockchain TEE, the blockchain enclave signature should reinforce OntoROPA signature.

- **PROACTIVENESS:** the date a ROPA is available is important from a legal perspective. The immutability properties of blockchain platforms will support this. The transaction associated to ROPA publication will provide proof of proactiveness.

2.1.3 Use case scenario

SCENARIO 1: ROPA CREATION. ROPA PROVIDERS CREATE ROPAS USING THE ONTOROPA APPLICATION.

A person responsible of ROPA creation and maintenance in an organization, for example, the responsible of data privacy in a university, needs to create and publish a ROPA to describe the personal data treatments in her university.
Her requirements are: to use standard vocabularies, to be sure that her ROPA includes the necessary information as required by article 30 of GDPR, and once this is achieved, to publish it and make it available to other ROPA providers, to data protection supervisors, and to the general public (this is mandatory for Public Administrations).
Moreover, she wants to be able to provide proof about the date the ROPA was published if the data protection supervisor authority (in Spain, the AEPD; in France, the CNIL, etc.) starts a procedure of inspection after

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

critical situations such as data breaches[4]. For this aim, the data privacy responsible uses the application that provides the forms to create a ROPA.
There are two main use cases:

1) ***Import ROPA***: A ROPA is already available as a pdf or excel sheet. This ROPA is imported.
2) ***New ROPA***: A ROPA is created from start.

We will extend on the second use case.

Use case: ***New ROPA***.
A ROPA provider wants to create a new RDF ROPA to describe the activities that deal with personal data in an organization. Figure 5 shows an overview of the process flow:

1) The first step is to create the RDF file that describes the ROPA.
2) The second step is to validate the ROPA, to check that it has correct information as requested by the GDPR.
3) Once it is ready for publication, its quality is certified.
4) The certified ROPA is published.

[4] Article … of GDPR stablishes the obligation to have available ROPA for inspections if requested by the data protection supervisor authority. Moreover, article… introduces the concept of proactiveness, which means that privacy by default and by design has been applied from the very start, that the security measures have been implemented from the very start, and that the information about the personal data activities is available. ROPAs are the records that collect this information. Therefore, ROPAs must be available at the same time than a personal data treatment starts. It is a concern of some data protection specialists that some ROPAs may be created after the supervisor request them.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

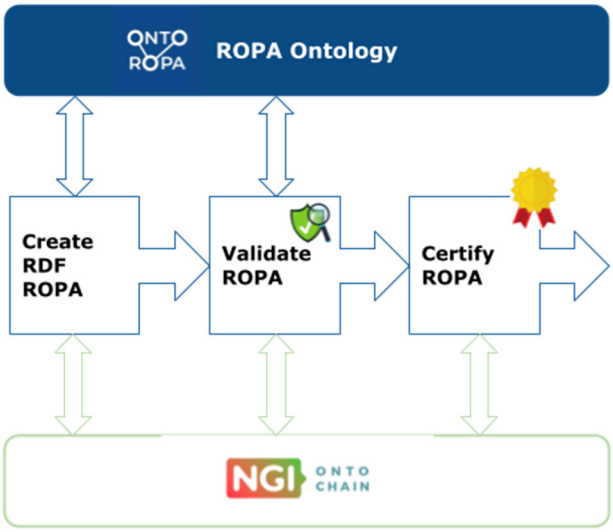

Figure 5. High level description of the use case New ROPA.

2.2 SOLUTION FUNCTIONALITIES

Functional requirements are collected in Table 1.

ID	Name	Description
FR1	Identity	Only users able to identify themselves as members of the ROPA creators community will be authorized to create ROPAs
FR2	Create ROPA	Create a new ROPA
FR3	Edit ROPA	Modify a ROPA
FR4	Delete ROPA	Erase a ROPA
FR5	Validate ROPA	Check the correctness of a ROPA
FR6	Sign ROPA	Sign ROPA with the digital signature of its creator
FR7	Certify ROPA	OntoROPA certifies the validity of a ROPA with its signature
FR8	Publish ROPA	A certified ROPA is published

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Table 1. Functional requirements.

2.2.1 Ontology Requirements Specification Document

During the OntoROPA project and implementation we will follow the Ontology Requirements Specification Document template set out in Suárez-Figueroa et al. (2008) as part of the NEON methodology for ontology development.

1. PURPOSE	
Standardization of ROPA definition as a knowledge model for reuse, interoperability and smart management of ROPA.	
2. SCOPE	
The knowledge represented in the ROPA Ontology includes the legal definition and requirements as described in Article 30 GDPR and the requirements derived by its implementation elicited from the community of privacy and data protection experts—mainly including lawyers, legal advisors and scholars, data protection officers, and rulers who are proficient in the creation and manipulation of ROPAs.	
3. IMPLEMENTATION LANGUAGE	
RDFS/OWL	
4. INTENDED END USERS	
A. Software developers to implement semantic-driven ROPA applications	
B. The community of privacy and data protection experts as standard language for representing ROPAs	
5. INTENDED USES	
A. Support ROPA generation/creation applications.	
B. Support ROPA validation/certification applications.	
C. Suport ROPA interoperability (exchange)	
D. Standardization of ROPA knowledge and data	
5. ONTOLOGY REQUIREMENTS	
A. NON-FUNCTIONAL	**B. FUNCTIONAL REQUIREMENTS**
Modularity	Competency questions (TbD during implementation).
Extensibility (Community)	Software requirements (use cases):
Expert-centred (practical knowledge)	**1 ROPA validation.** Allow the validation of the ROPA data against the knowledge model for completeness and correctness.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Legal-compliance and correctness (art. 30)	**2 ROPA description.** Offer a complete description of ROPA to suport the creation of compliant GDPR ROPA.
6. METHODOLOGICAL APPROACH	
We take into account the detailed modelling guidelines from Noy & McGuinness (2001) and Fernández-López et al. (1997), but include expert-centred and empirically-oriented methods towards professional legal knowledge acquisition, and usability (shareability) evaluation towards the construction of the ROPA Ontology. The methodological steps will follow the general cyclic iterative and incremental approach: specification of requirements, knowledge acquisition, conceptualization, formalization, evaluation and refinement. **Evaluation:** • Expert Verification: Verify the correctness of the competency questions with experts. • SPARQL demonstration: create a SPARQL competency question query with demonstration data from an existing ROPA .	
7. SOURCES OF KNOWLEDGE	
A. ROPA Experts Survey	D. Ontology reuse
B. GDPR and other related regulations	E. Data - Public administration ROPAs
C. Expert input (e.g. Ontoropa Expert input, Focus groups, etc.)	

2.2.2 Software Requirements Specification

Data requirements

1) **ROPAs:** ROPAs contain the information about personal data treatments, as requested by article 30 of GDPR. They will be represented as RDF graphs.
2) **Ontology:** The OntoROPA ontology collects knowledge about ROPAs. The ontology will cover knowledge extracted from GDPR and expert knowledge. It will be an OWL ontology.
3) **Verifiable credentials:** They will be used to authenticate users. Users can be individual persons, or organizations. A user can have multiple credentials, per community and organization. Each credential determines the role the user has in a community as a member of the organization that signs the credential.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Non-functional requirements: security, privacy, others

ID	Name	Description
NFR1	Availability	The service should be available 90% of time. It is not critical.
NFR2	Ease of use	95% of ROPA providers should be able to use the service after a brief tutorial
NFR3	Design	The design guidelines of OntoROPA and ONTOCHAIN should be applied
NFR4	Storage	An RDF store should be used to store the RDF graphs. If available, one able to trace ROPAs history in a trustworthy manner from the ONTOCHAIN ecosystem.
NFR5	Secure execution of validation	The validation process should be protected from external injections
NFR6	Ontology-based validation	The validation will use an ontology, the OntoROPA ontology
NFR7	Digital certificates	Digital certificates should follow the X509 standard
NFR8	Privacy by design/Privacy through Design	The identity of ROPA creators should be linked to their professional role, and her relation with an organization. No personal data should be available to other users. An additional monitoring conflict resolution system could

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

		be added on top of that to ensure compliance with GDPR requirements (consumers' rights)

Table 2. Non functional requirements

Data flow – Interaction diagrams for the *New ROPA* use case

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

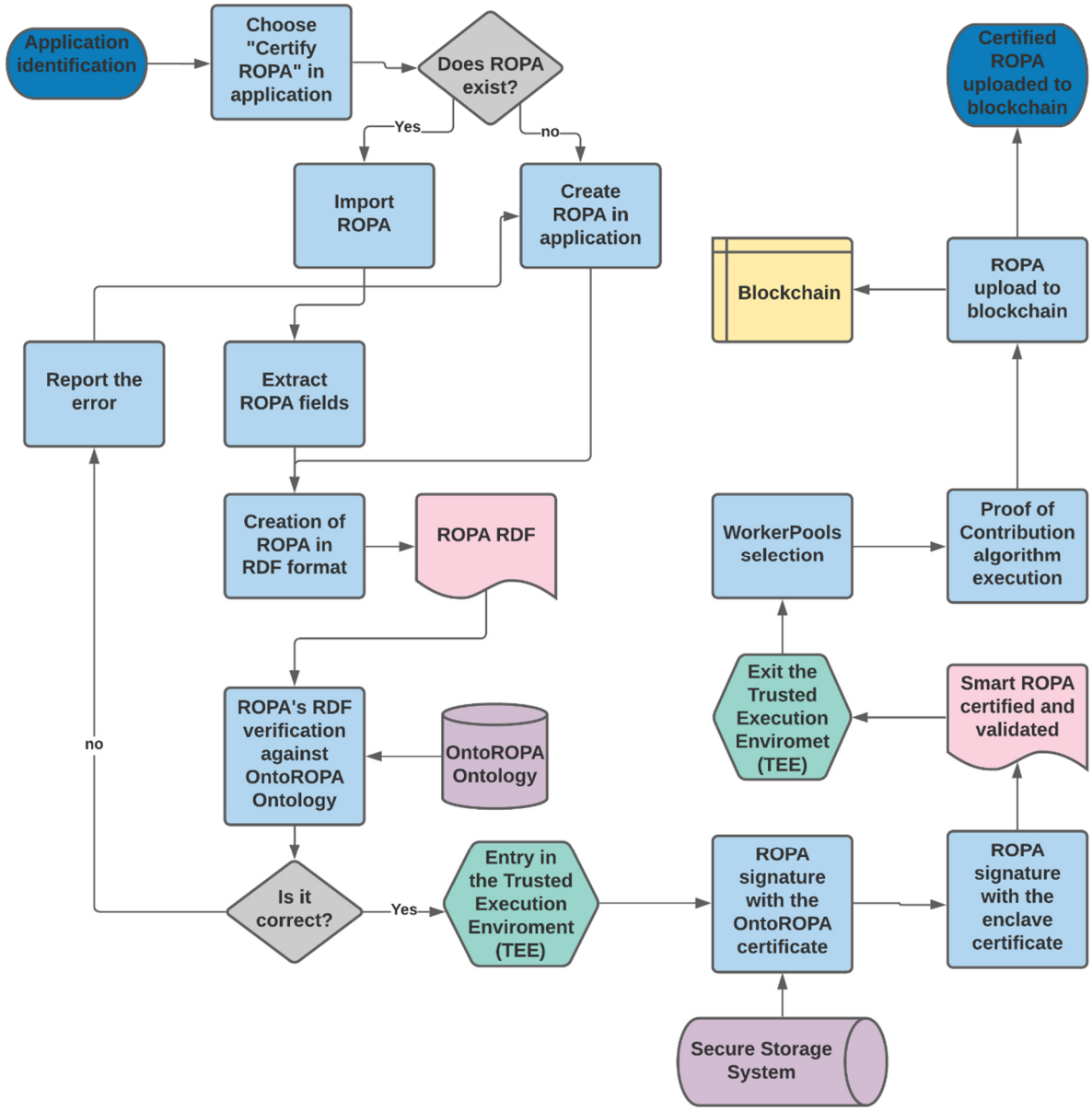

Figure 6. Flowchart for the New ROPA use case.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

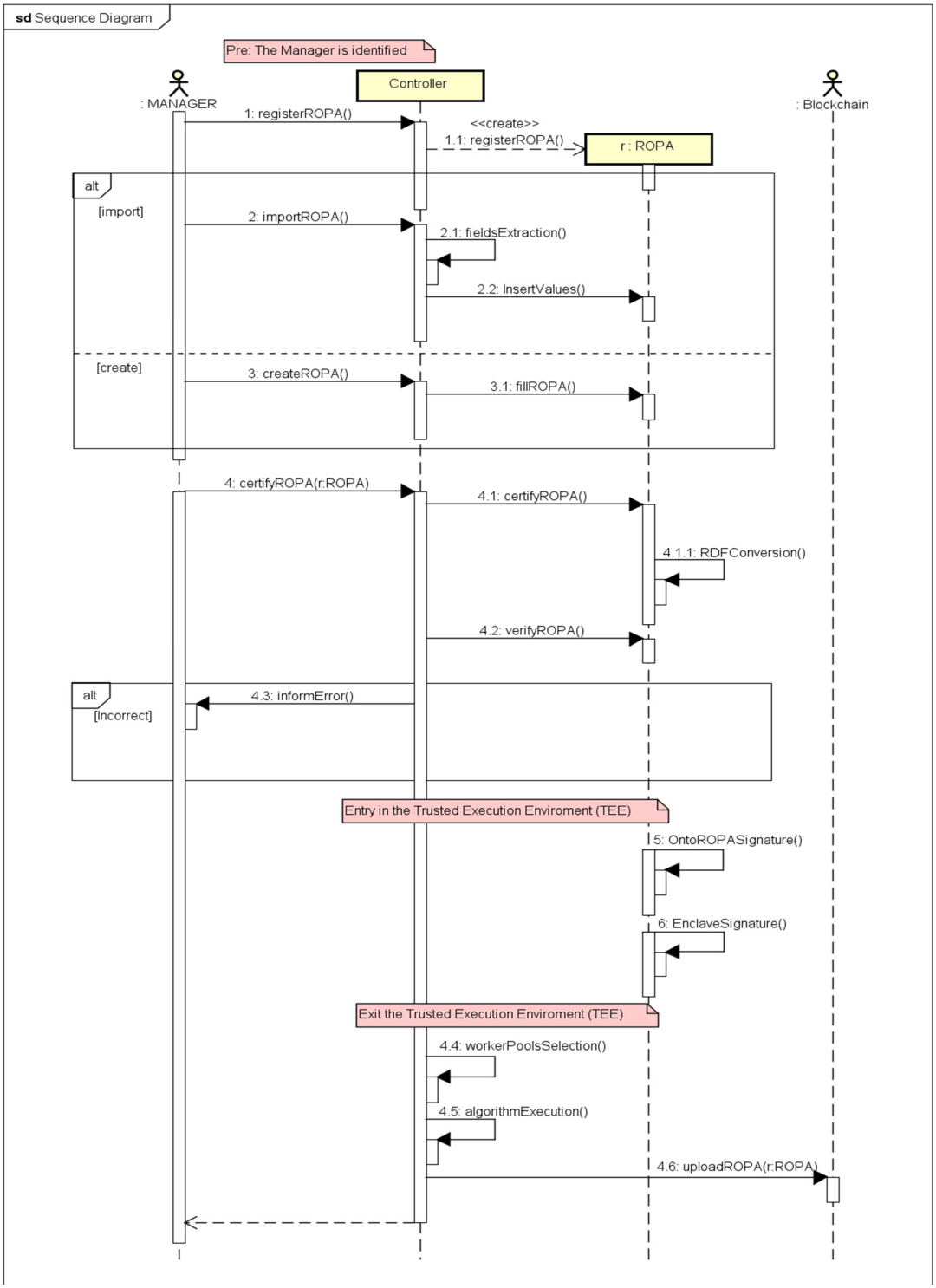

Figure 7. Sequence diagram for the New ROPA use case.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

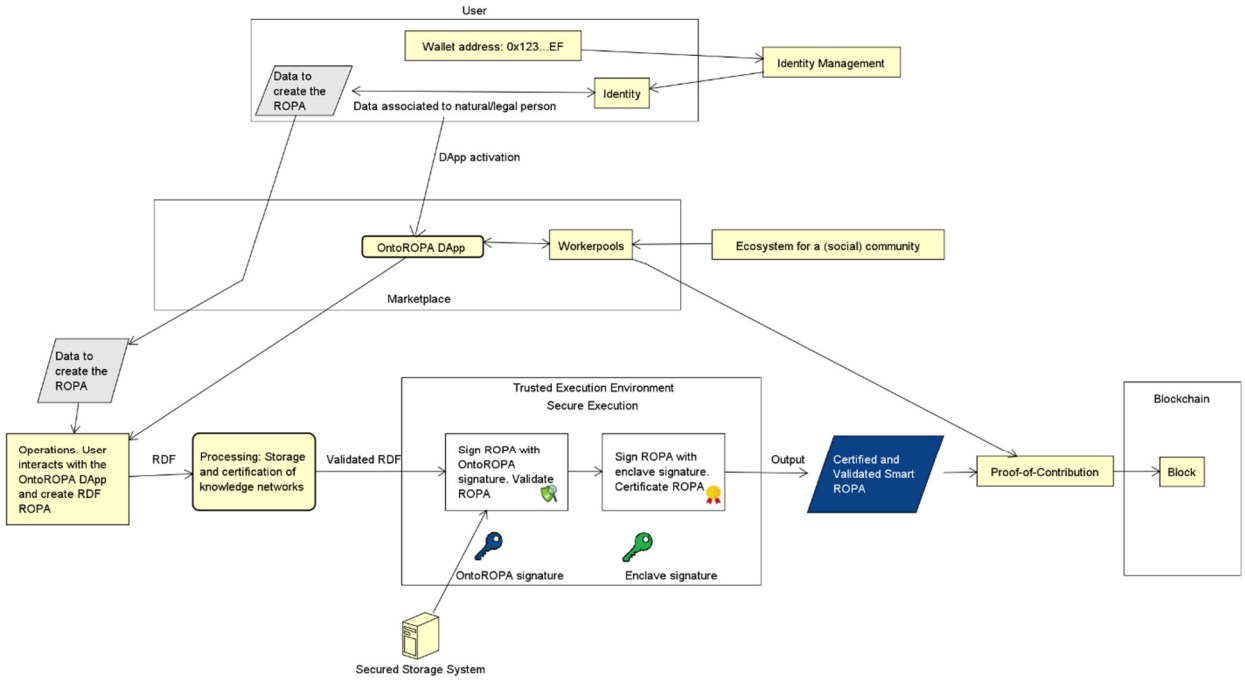

Figure 8. Data flow for the New ROPA use case.

2.3 INTERFACES WITH THE OTHER ONTOCHAIN BLOCKS

The envisaged synergies for the OntoROPA New ROPA use case are aligned with the module architecture of OntoROPA. This modular approach will facilitate OntoROPA **resilience to changes in collaborators**. For example, we can either take in charge the Identity module with the development of **our own oracle**, able to validate X509 digital certificates in LDAP

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

services (a proof of concept is already done, see Figure 10 for an extract of data about the certificates generated), or to use services provided by HIBI and/or SSiVault. Figure 9 shows the synergies for this use case. The synergies we envision are summarized in table…

Service	**ONTOCHAIN block**
Identity	HIBI and/or SSiVault
Community management	SEIP
Qualified RDF storage	GraphChain
(Certification of) Trusted execution	KnowledgeX and/or iExec TEEs
ROPA provenance (certification)	GraphChain

Table 3. OntoROPA synergies with ONTOCHAIN blocks.

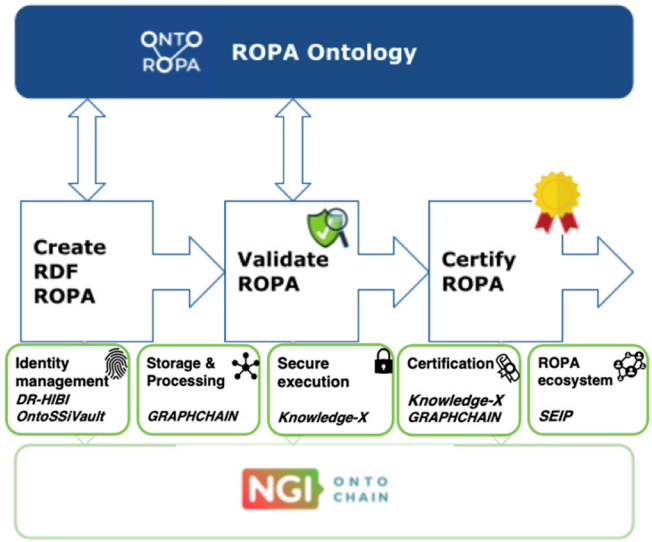

Figure 9. Synergies for the New ROPA use case.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

2.3.1 Interaction with other ONTOCHAIN blocks

Smart contracts seem to be the appropriate means of interaction in a blockchain ecosystem. The OntoROPA smart contract will include the invocation to each of them as convenient. The detailed design will be tackled once we know what are the applications we can work with.

2.3.2 Data exchanged with other ONTOCHAIN blocks

VERIFIABLE CREDENTIALS FOR USERS IN ROPA COMMUNITIES

Verifiable credentials will be exchanged with SEIP communities management system. Moreover, these credentials will be provided to the ONTOCHAIN members able to deal with digital identity, that is, to receive a credential and return a {valid | not valid} result. ONTOCHAIN teams dealing with digital identity are HIBI and SSiVault.

Table 4 summarizes the main data in a verifiable credential for the New ROPA use case. The role that a user has in each community determines the grants (permissions) she has in the community.

ORGANIZATION:	**OntoROPA**
COMMUNITY, C:	ROPA providers (referred to as "Privacy" in the example of figure 2)
USER, U:	Responsible of data privacy in Organization OU
ORGANIZATIONAL UNIT that authorizes user U as ROPA provider in the community:	OU

Table 4. Data about participants in an OntoROPA verifiable credential.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

There is a certificate for each user and community (User, Community). The data model is the one in Figure 10. Figure 11 shows a proof of concept with the "Privacy" community of OntoROPA.

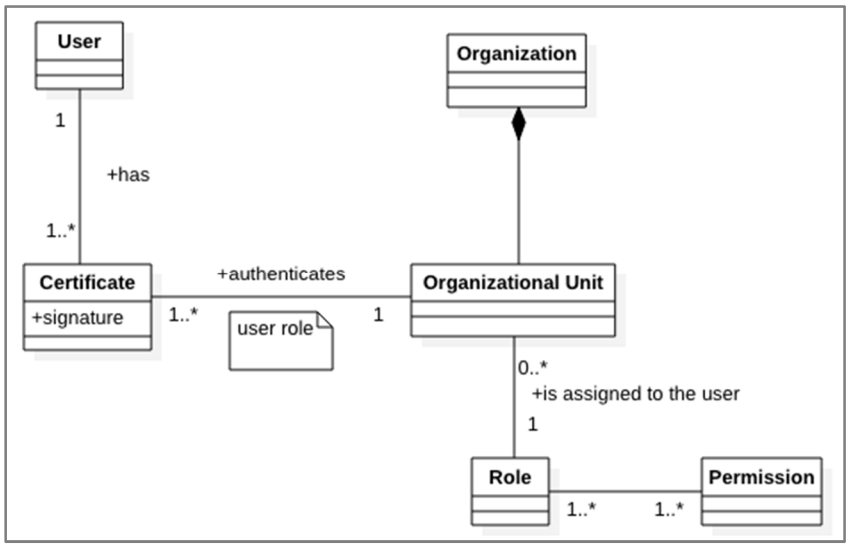

Figure 10 Data model for credentials of users of OntoROPA communities.

```
root@4ck:/etc/ssl/certs# openssl x509 -in ontoropa.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            78:a4:30:6a:01:36:f4:9a:fc:01:68:6c:0e:5b:81:0c:37:52:ec:9e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = ES, ST = Palencia, L = Palencia, O = OntoROPA, OU = Privacidad,
CN = ontoropa.local, emailAddress = ontorora@ontoropa.com
        Validity
            Not Before: May 16 20:37:41 2021 GMT
            Not After : May 16 20:37:41 2022 GMT
        Subject: C = ES, ST = Palencia, L = Palencia, O = OntoROPA, OU = Privacidad,
CN = ontoropa.local, emailAddress = ontorora@ontoropa.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
```

Figure 11. Example of certificate for the OntoROPA Privacy community

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

3 IMPACT

3.1 BUSINESS MODEL DESCRIPTION

OntoROPA's business model is a pre-business plan definition that allows us to clearly define what we're going to offer the market, how we're going to do it, and how OntoROPA could generate revenue.

Competitive Advantage: Provide a regulatory model designed specifically for the implementation of OntoROPA in the data market. The OntoROPA Regulatory Model will be a strong governance mechanism to ensure that the project strikes the right balance between expected progress and innovation, and aligning research activities and the OntoROPA ecosystem with relevant ethical and legal requirements and social values

Growth plan: As there is no pre-established business model with these features OntoROPA will have an economic reserve to expand.

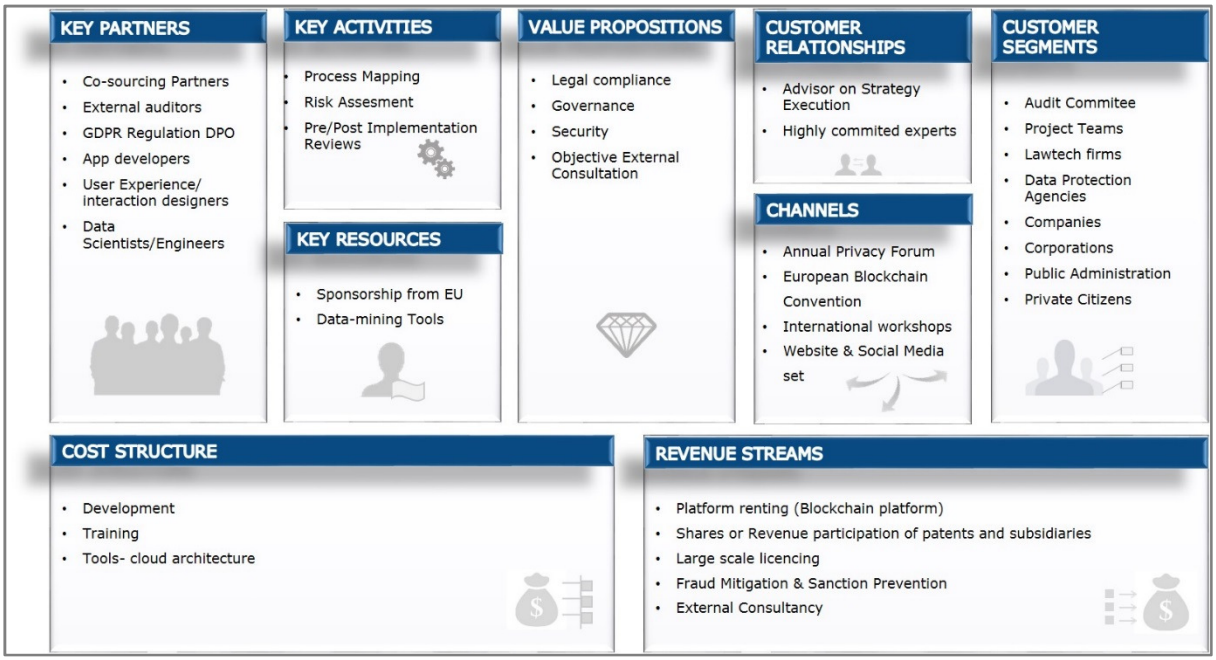

Figure 12. OntoROPA Business Model Canvas.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

3.2 BUSINESS VALUE FOR ONTOCHAIN

It is important for business to look to technology to address the dual challenges of legal compliance and effective information management.

Legal Compliance is essential in organizations to ensure compliance with their Codes of Conduct, as consumers demand products and services provided from "ethical and sustainable" behaviours and access Social Networks to publicly denounce those companies that do not meet their commitments, resulting in serious reputational damage and significant sales drops.

Non-compliance with these obligations is punished with a range of criminal and administrative sanctions ranging from heavy fines to professional disqualification or cessation of activity, as well as irreparable reputational damage.

Return on Investment in legal compliance

Digitization provides tools to develop compliance policies but also leads to new regulatory demands that complicate their implementation.

But at least companies have become aware of the many benefits of the determined and visible commitment to a culture of "compliance". They range from circumvention of sanctions to improving the working climate, from fraud and corruption prevention to reputational improvement.

Although it is considered a cost in many cases, legal compliance is actually an investment of organizations, which allows it to make the business profitable by implementing an effective working methodology, based on prevention and making better decisions.

There are three indicators that can help quantify a return on investment in legal compliance:

1. **Increased competence and efficiency within the organization.**

   When a legal compliance system is integrated into the organization, processes and controls are implemented to standardize the operation according to good legal compliance practices. These good practices go beyond "complying with the law" and often adopt international standards. This standardization contributes to greater efficiency particularly in production processes.

2. **Savings by reducing legal risks and prevention of sanctions.**

   The materialization of a legal risk can have such an impact that it can cause any medium or small business not being able to withstand large sanctions and their associated expenses. When

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

calculating the cost of implementing and maintaining OntoROPA system, it is foreseen that this will usually be a minimal fraction of what would represent the economic impact of a penalty (and the expenses associated with the incident).

The difference between the cost of OntoROPA and the maximum impact suffered from not having the right controls in place is money that has saved your organization's compliance function.

3. **Generation of new and better business opportunities.**

The results of the surveys in which experts have participated show us the formal evidence that companies spend too much time on issues that could be done more effectively. With this standardized and automated tool, Ontochain can provide consulting services specializing in data protection, such as risk assessment, compliance with ISO 27001 and ENS.

ROPA controllers will benefit from having a standard tool to simplify the task of creating their own ROPAs, and the possibility to adapt/extend it to their own use cases.

The main objective will be offering OntoROPA as a legal web service for all stakeholders (including Law Tech firms, data protection agencies, companies, corporations, and private citizens.)

3.3 RELEVANCE TO BLOCKCHAIN IN GENERAL AND ONTOCHAIN IN PARTICULAR

OntoROPA's ambition is to innovate in checking and monitoring legal compliance, using blockchain technology to demonstrate that it can also be used for privacy compliance in the new Law Tech market.

Innovation in legal compliance will be achieved by providing legal value to digital artifacts and procedures created to comply with legal data protection requirements at regional, national and European levels. This is something that current tools in the legal compliance market do not provide.

Blockchain technology has been questioned by privacy experts, editors, and rulers because its distributed nature is not fully compatible with GDPR requirements. OntoROPA will provide Blockchain technology with ways to address problems that have arisen and remove technical and legal barriers. In addition, in doing so, it will create a specific niche market, generating a safe and reliable legal ecosystem with economic value.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

The legal perspective we are adopting to make this a reality is the specific version of the rule of law focused on the protection and enactment of substantive rights. This means that transactions, data governance, and procedural rules contained in binding provisions such as the European GDPR can be modelled in such a way that (i) all stakeholders can participate, (ii) ensuring a legal space in between government, administration, the market, and end-users' interests. I.e. a space for legal governance. This is what ONTOCHAIN will deliver, as main component of the digital infrastructure (and data sovereignty) for the new platform-driven economy of the European digital market.

3.4 SOCIETAL IMPACTS: TECHNOLOGICAL, SOCIO-ECONOMICAL, ENVIRONMENTAL

Law Tech has created an expanding legal market, in which companies offer a variety of legal services mainly based on AI and machine learning solutions—not just the more traditional e-discovery but supervision, monitoring and automatic compliance of regulatory systems, including smart contracts, cryptocurrencies and online dispute resolution. However, it still is a volatile market. Just before the last pandemic, Law Tech venture capital investments increased dramatically at the rate of 2.4 new start-ups per day (Casanovas, 2021).

The automation of legal documents is the most well-trodden path. Legal compliance is the least—as it certainly is a more complex relational field, because the behaviour of all stakeholders must be taken into account (not just meaningful texts to be interpreted).

There are systems in legal informatics that have been designed for drafting, storing, organising, consolidating, or retrieving provisions in plain natural language to eventually support legal decision-making (Boella et al., 2013). However, turning norms from natural to formal languages combining NLP techniques and defeasible logic is a difficult task (Wyner et al., 2013). This has not yet been completely solved. The current research is focusing on how to semi-automate the extraction of norms and their elements to populate legal ontologies, combining state-of-the-art general-purpose NLP modules with pre- and post-processing using rules based on domain knowledge to solve the so-called "resource bottleneck problem". Thus, trying to semi-automate the extraction of definitions, norms, and their elements to reduce the need of human intervention (Humphreys et al., 2020). This is a conceptual challenge, lately also called Rules as Code in e-government administrations (Waddington, 2020; Governatori et al., 2020).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

OntoRopa is benefiting from this expanding market of legal web services. The solution for modelling ROPAs fits into the legal compliance modelling landscape, but we think it is simpler, and easier to be understood, accepted, and adopted not just by Law Tech companies, lawfirms and corporations, but by official drafters, rulers, controllers, and supervisors. There is a need to comply with GDPR requirements. Hence, OntoRopa can be expanded through a variety of legal ecosystems, depending on the private or public field of deployment.

Most important, the OntoROPA approach fits nicely into the specific privacy market that will be developed in the European Union in the immediate future. The new strategy mindset represents a shift in the EU's focus, from protecting individual privacy to promoting data sharing as a civic duty. There are initiatives (e.g. the TRUSTS project) to create a pan-European market for personal data through a mechanism called a data trust, a steward that manages people's data on their behalf and has fiduciary duties toward its clients. We do not yet know whether and how this market will be effectively developed, but certainly the solutions provided by OntoROPA are most needed to implement it.

As Acquisti et al. (2016) underline, "it is abundantly evident that protection of personal privacy is rapidly emerging as one of the most significant public policy issues, and research on the economics of privacy will, therefore, continue to expand and evolve in coming years. Thus, it stands to reason that, case by case, diverse combinations of regulatory interventions, technological solutions, and economic incentives, could ensure the balancing of protection and sharing that increases individual and societal welfare."

3.5 LEGAL VALUE FOR ONTOCHAIN

OntoROPA will ensure that all the automated processing carried out to create, handle, store and retrieve ROPAS is compliant with the law. Legal validity (i.e. 'legality') is not equivalent to computational or logical validity. ROPA validation refers to the accuracy, traceability and technical reproductivity of the process that has generated it. It will be reached through the ontology.

However, this is not turning ROPAS into valid processes with legal outcomes and effects. Automated legal validity should be carried out aligning: (i) the selection of relevant legal sources in a transparent, shareable, and acceptable way, according to the main legal doctrine, (ii) the normative interpretation process that is accepted by official bodies, such as Data Protection agencies, (iii) as a last resort, the normative interpretation process that is accepted by regional, national

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

and European judiciaries. There are a variety of normative and regulatory sources that should be taken into account.

To ease the process of handling them we have defined them into four legal different clusters: (i) Hard law (laid down by Parliaments and the Judiciary (this includes European Regulations, such as the GDPR, and the Directives that have been transposed into the national legal systems by the State members); (ii) soft law (such as international agreements and covenants, mandatory after mutual or collective agreements); (iii) policies (issued by European and national governments to developing, enforcing, and implementing Acts, Regulations, and case-based law sentences), (iv) ethical principles and values, as they have been discussed, proposed and accepted in specific sectors (such as the recent EU guidelines for Artificial Intelligence).

OntoROPA use cases are primarily focused on the Spanish case. Thus, in addition to GDPR, European policies, and international ISOs, applicable Spanish legislation will be also analysed to fully understand the handmade ROPAs generated by the person in charge ('responsible person') or by her deputy. Spanish legislation specifies the content of the data to be handled and differentiates between the responsible (officer) of data protection treatment and her (appointed) deputy (art. 30 LOPD). The structure and content of the ROPA transcribed in Section 2 can be understood in light of art. 31 of the Spanish Data Protection Act[5] , which lays down the added requirement of stating the legal ground of the information being certified:

> The subjects listed in article 77.1 of this Organic Law will make public an inventory of their treatment activities accessible by electronic means, which will contain the information established in article 30 of Regulation (EU) 2016/679 *and its legal basis.*

[5] *Ley Orgánica de Protección de Datos*. Artículo 31. Registro de las actividades de tratamiento. 1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5. El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro. 2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal. *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Besides legislation, it is worth noting that the legal value—i.e. *legal validity*—is created through a process that fosters legal security and social trust among all stakeholders in the market (including companies, corporations, administrations and citizens). Then, ISO standards and technical protocols (such as the W3C standards and recommendations) matter.

As stated by EU recent strategies, better regulation principles involving Impact Assessments and citizens' consultations, and the introduction of digital currencies as a basis for the EU digital market fosters the general use of specific policies and best practices that benefit from the experiences already gathered. A Pan-European blockchain regulatory sandbox, and a *Markets in Crypto-Assets Regulation*—MiCA— are on the way. They will intend to support innovation while protecting consumers and the integrity of crypto-currency exchanges (no insider trading, front running etc).

The legal value of these exchanges must be assessed, focusing on *digital transactions*. Doing so, regulatory tools become more complex and granular, leading to the notion of *legal governance* to refer to all regulatory components that should be put in place to build the legal validity—i.e. the *legality*—of the exchanges. Beyond the usual definition in business compliance modelling, legal governance can be defined as the mindset of all computational and systemic (organisational) instruments that are required to generate legal ecosystems, i.e. the sustainable regulatory framework in which digital transactions take place fostering security, trust and institutional strengthening.

OntoROPA embraces the *middle-out approach* to AI governance set by the AI4People Report to the EU Parliament (November 2019).[6] It can be defined as the middle-ground between top-down and bottom-up regulatory approaches, fostering co-regulation, co-responsibility and dialogue between rulers and the subjects of regulation (Pagallo, Casanovas, Madelin, 2019). Figure 13 plots OntoROPA legal governance system. Figure 14 draws its different layers and dimensions. Figure 15 shows OntoROPA legal ecosystem.

[6] https://www.eismd.eu/wp-content/uploads/2019/11/AI4Peoples-Report-on-Good-AI-Governance_compressed.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

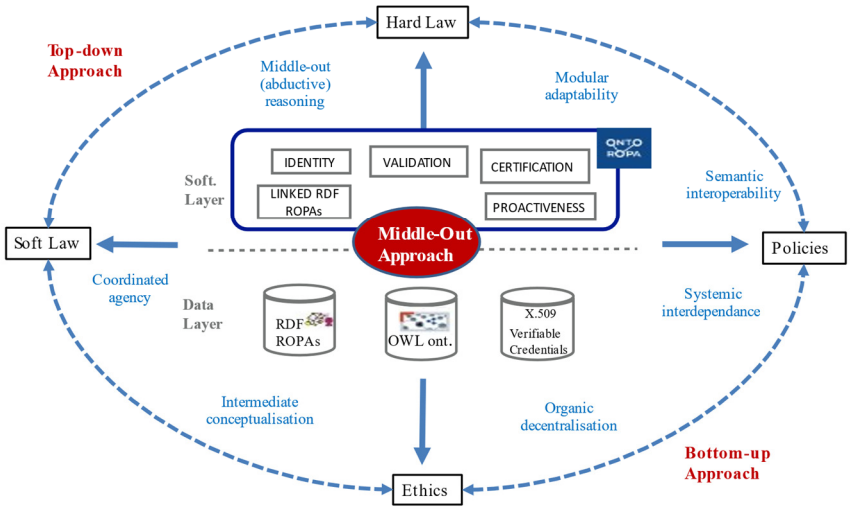

Figure 13. OntoROPA Legal Governance System.

It is worth mentioning that law or its digital version, legal governance systems, do not constitute in OntoROPA a third layer on top of the data layer and the software layer defined above (section 2). There is no legal layer consisting mainly in documents that can be deemed 'legal'. What it does exist instead is a dynamic set of normative systems, guidelines, values, policies, standards and best practices that integrate a complex cognitive system embedded into human behaviour and (now) information systems.

This dynamic set constitutes a *dimension* of human and artificial systems and interfaces. It pervades the software and the data layer *from inside out*. This is why a middle out approach can be the most appropriate to generate the legal ecosystem that is needed to validate ROPAS and ROPAS' computational management in both senses—technological and legal. There are two layers—software and data layer—and three dimensions—technological, social, and legal. The links between them occur stemming from the secured process to produce a certified and legally valid ROPA.

The OntoROPA legal ecosystem is generated by the set of technical requirements and social and legal conditions that are taken into account by controllers, supervisors, professional agents in the marketplace (legal web services, law firms and companies). Thus, the certification and validation processes involve the participation of all stakeholders. Again, technical requirements do not reflect per se the social and legal

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

conditions: they are reached through (i) the mutual understanding of regulations, i.e. the shared agreement on the rights and duties set by the regulatory system (legislation, policies, best practices, and ethics), (ii) the mutual understanding of the position of all agents participating in the process, (iii) the mutual understanding of all necessary actions to be taken to make the final product 'legal'. This is where the legal validity of certification comes from. Certification and validation processes do not stand by their own: they are necessary components of the legal ecosystem generated through the coordination of all required elements, as shown by Figure 14.

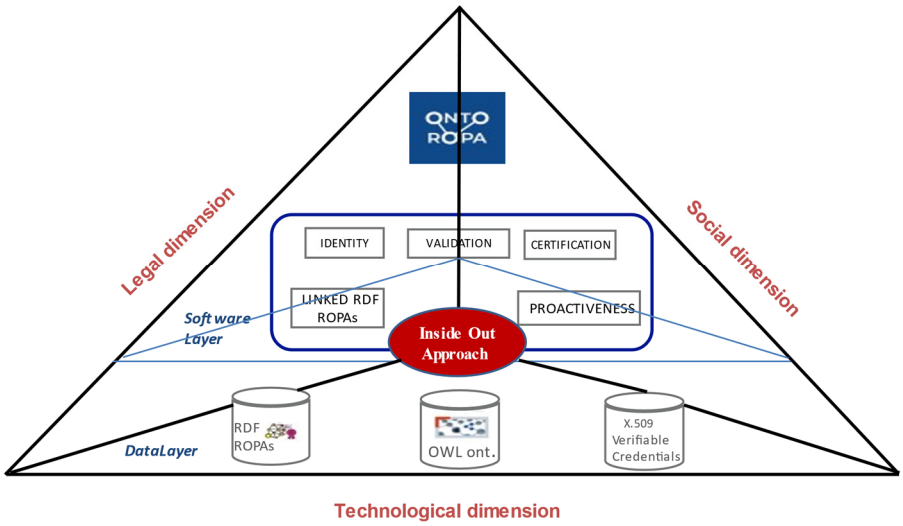

Figure 14. Inside-out Approach: OntoROPA dimensions and layers.

Figure 15 shows the architecture of OntoROPA legal ecosystem. Certified and validated ROPAs are followed by a proof of contribution and a smart contract linking users, controllers, and supervisors, in between blockchain and the community of users.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

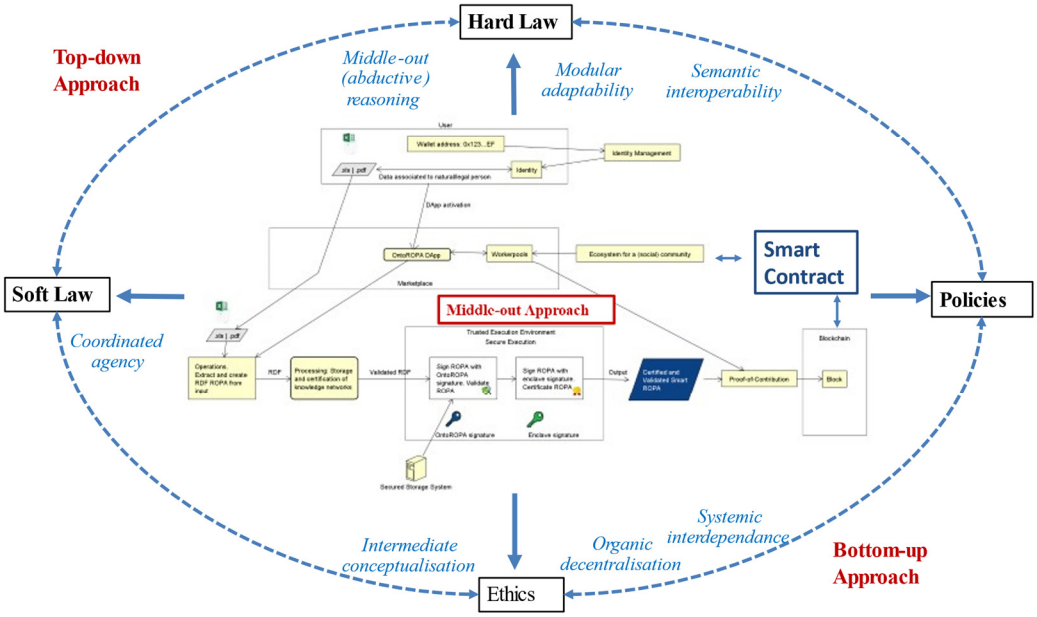

Figure 15. OntoROPA Legal Ecosystem.

The use of blockchain technologies has generated some controversies about its compatibility with GDPR requirements. As assessed in OntoROPA Deliverable 1, permissionless blockchains are distributed, decentralised peer-to-peer networks in which everyone can participate interacting with unknown counterparties, trusted or not. The clear allocation of responsibilities that is required by GDPR are not present in this situation, as assessed by Michèle Fink's study for the European Parliament on blockchain and data protection (Fink, 2019). The study recommends closing agreements between regulators and the private sector, and the elaboration of codes of conduct and *certification mechanisms* for blockchain technologies that should be "compliant by design". Table 1 summarises the legal risks at stake, as set by the French *Commission Nationale de l'Informatique et des Libertés* (CNIL) *participants* analysis of the situation, and the solution provided by OntoROPA. We do not have the solution yet for all the issues, but focusing on transactions and having in mind the certification process helps to sort them out.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Privacy problems in Blockchain	Legal Risk	CNIL Recommendation	OntoRopa
Identification of Data Controller	All participants may be qualified as data controllers when the processing is related to a professional or commercial activity (i) as natural persons, (ii) as legal persons, (iii) as "joint controllers".	To identify the data controller in advance (a representative or a legal person).	**Data controllers are identified in advance**
Identification of Data Processors	In blockchain, smart contract developers and miners are deemed to be processors under GDPR	Processors and miners should establish a contract with the participant acting as data controller which specifies each party's obligations	**This has been planned**
Identify the reasons to use blockchain solutions over other possible instruments	Not to comply with all requirements and safeguards set by GDPR	Favouring other solutions that allow for full compliance with the GDPR.	**OntoROPA endorses some security solutions which are deemed to be fully compliant**
Consider the requirements that affect data transfers outside the EU	The requirement for appropriate safeguards for transfers outside the EU, such as binding corporate rules or standard contractual clauses, are entirely applicable to permissioned blockchains	Permissioned blockchains should be favoured as they allow a better control over personal data governance.	**This has been planned**
Carefully choose the format under which the data	In blockchain, the data registered on a blockchain cannot be	Some technical solutions should be examined by stakeholders in	**This can be changed in a successive transaction**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Privacy problems in Blockchain	Legal Risk	CNIL Recommendation	OntoRopa
will be registered	technically altered or deleted once a block in which a transaction is recorded has been accepted by the majority of participants.	order to solve this issue.	
Identifiers of participants and miners	The architecture of blockchains means that these identifiers — alphanumeric characters which constitute the public key linked to a private key, known only by the participant— are always visible.	This data cannot be further minimised and that their retention periods are, by essence, in line with the blockchain's duration of existence.	**Identifiers can be protected under the Spanish law**
Additional data (or payload) stored on the blockchain containing personal data related to other individuals	The GDPR principle of data protection by design requires the data controller to choose the format with the least impact on individuals' rights and freedoms.	The CNIL considers that personal data should be registered on the blockchain preferably in the form of a *commitment*[7], or alternatively in the form of a hash generated using a hash function with a key, or, at least, in the form of an encryption ensuring a high level of confidentiality.	**Commitments and hashes are under study. We prefer the principle of "data protection *through* design" to monitor the human-machine interfaces**
To ensure the effective	The GDPR was designed to give individuals back	The format chosen to register the data on a	**Partially solved (we still must have an answer for the issue raised by the right to**

[7] A "commitment" is a cryptographic mechanism that allows one to "freeze" data in such a way that it is both possible - with additional information - to prove what has been frozen and impossible to find or recognise such data by using this sole "commit".

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Privacy problems in Blockchain	Legal Risk	CNIL Recommendation	OntoRopa
exercise of rights	their control over personal information. The right to erasure, the right to rectification and the right to object to a blockchain are difficult to apply in blockchain.	blockchain can also facilitate the exercise of individual rights.	**counterbalance what has been recorded).**
Compatibility of rights	The GDPR rights of information, of access and of portability are not problematic.	The data controller must provide concise information that is easily accessible and formulated in clear terms to the data subject before submitting personal data to miners for validation.	**Granted**
Incompatible rights	It is technically impossible to grant the request for erasure made by a data subject when data is registered on a blockchain	However, when the data recorded on the blockchain is a commitment, a hash generated by a keyed- hash function or a ciphertext obtained through "state of the art" algorithms and keys, the data controller can move closer to the effects of data erasure using *commitment schemes*[8] and	**Granted**

[8] "When a commitment scheme is perfectly hiding, deleting the witness (i.e. the element that allows to verify that a given value is committed in a given commit) and the value committed is sufficient to render the commitment anonymous in such a way that it can no longer be considered personal data".

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Privacy problems in Blockchain	Legal Risk	CNIL Recommendation	OntoRopa
		deletion of the keyed hash function's secret key.	
Security requirements	The different properties of a blockchain (transparency, decentralisation, tamper-proof and disintermediation) mainly rely on two factors: the number of participants and miners, and on a set of cryptological mechanisms.	For permissioned blockchains, the CNIL recommends: (i) Carrying out an evaluation of the minimal number of miners which would ensure the absence of a coalition that could control over 50% of powers over the chain; (ii) setting out technical and organisational procedures to limit the impact of a potential algorithm failure (including an emergency plan); (iii) the governance of changes to the software used to create transactions and to mine should be documented (ensuring an alignment between planned permissions and practical application).	**Under study, but CNIL recommendations are going in the OntoROPA direction of "compliance through design"**

Table 5. Blockchain and privacy CNIL and OntoROPA solution

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

4 IMPLEMENTATION

4.1 FEASIBILITY AND MODULARITY OF THE SOLUTION

4.1.1 Ontology Modularity

Large ontologies may suffer from reusability, scalability and maintenance issues. There are several ontology development approaches that overcome these issues: ontology modules, ontology extensions and pattern-based ontologies.

All these approaches focus on developing components or building blocks that together conform a larger ontology. "An ontology module is a reusable component of a larger or more complex ontology, which is self-contained but bears a definite relationship to other ontology module" (Doran, 2006).

This implies that ontology modules can be reused by themselves, in combination, or by extending them with new classes or properties.

The OntoROPA ontology development approach will take into account the legal and practical competency questions to establish and develop ontology building blocks that will allow extensions for reuse and maintenance. Furthermore, the project aims at providing extension guidelines for experts to ensure the ability of the ontology to evolve according to data protection practice principles.

As noted by Blomqvist (2004) "a problem with reusing an ontology can often be that the developer has no way of knowing what parts can be discarded and how the different parts depend on each other".

Therefore it is important that the OntoROPA ontology is developed with reuse in mind, so that for example modelling decisions and assumptions are made explicit and the development process is structured in a way so that its reuse can be incorporated in a well-defined way (Blomqvist, 2004).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

4.1.2 Software modularity.

The OntoROPA modules are as follows:

1) Identity

2) Linked RDF ROPA

3) Validation

4) Certification

5) Proactiveness

See section 2.1.2 for more details.

4.2 REAL TIME PERFORMANCE OF THE SOLUTION (KPI AND EXPERIMENTAL EVALUATION)

4.2.1 Ontology KPIs

We have established two different sets of ontology KPI: development and implementation.

Ontology Development KPIs		
Ontology Quality		
KPI Timeline	*KPI Description*	*Measurement*
6 months	Expert validation and approval of the ontology models and patterns developed from competency questions.	In-house data protection expert evaluation – approval
3 years		Focus group evaluation – approval SPARQL validation success
Ontology Coverage		
KPI Timeline	*KPI Description*	*Measurement*
6 months	Coverage of the competency questions that have been modelled as semantic knowledge.	25.00%
3 years		100.00%

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Ontology Implementation KPIs		
Ontology Adoption – Services		
KPI Timeline	*KPI Description*	*Measurement*
6 month	Encourage services and applications to integrate the OntoROPA ontology as part of their architecture (documentation and traning materials).	OntoROPA applicatio
3 years		3 services/applications
Community Growth		
KPI Timeline	*KPI Description*	*Measurement*
6 months	Build a ROPA community for ontology maintenance and extension (similar to EuroVOC principles	Community interactions mock-up with OntoROPA experts and focus groups
3 years		System to provide access to community members and change requests and extension development guidelines.

Table 6. Ontology KPIs

4.2.2 Software KPIs

The explored way in OntoROPA for improving processes is based on scorecard approach. Key Performance Indicators (KPIs) accommodated in scorecards is an usual tool within the strategic management, but is rarely used effectively in the field of software projects, which are more commonly evaluated by productivity assessment metrics linked to the generation of code as the "number of lines of code" or "function points" This work aims to identify and define a collection of Key Performance Indicators which allows effectiveness to be measured in this supply-chain context. The different key indicators are conveniently set in a specific scorecard that allows decision making associated with top level project management.

Key Performance Indicators (KPIs) help understand how good the performance is in relation to the strategic goals and objectives.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

The set of proposed KPIs are:

KPI	Description	Metrics		
Leadtime	how long it takes to go from "idea" to delivered software	12 months		
Cycletime	how long it takes to make a change to the software system and deliver that change into production	1 month		
		Monthly	Yearly	Average
Efficiency/Performance	Capacity and Functional stability	100%	95%	100%
Security	Integrity & authenticity	100%	95%	98%
Code Readability	Data Structure	100%	95%	98%

Table 7. Software KPIs

4.3 INTEROPERABILITY ASPECTS

4.3.1 INTEROPERABILITY IN DATA AND KNOWLEDGE

Davies et al. (2020) rightly emphasise how our society becomes increasing reliant upon 'data-driven' approaches to the delivery of services in both business and government, and consequently the importance of achieving semantic interoperability, at scale, should be clear enough.

In this line, the Ontoropa team is particularly focused on the issue of the lack of interoperability in current representation and management of ROPAs. Most of these records are created and published as pdf or excel files. They are not interoperable, neither syntactically nor semantically. It is impossible to apply AI or other methods capable of inferring new knowledge from the data if the semantics are not available for automatic processing.

The challenges for OntoROPA in this area are twofold:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

- To develop a reliable and transparent approach to managing access to ontologies, metadata, knowledge and information, providing technical solutions based on successful semantic web approaches such as Linked Data and OWL.
- Offer ontology-based solutions to validate the logical consistency of ROPA.

The use of Semantic Web standards and the application of Linked Open Data principles to represent ROPAs will allow them to be managed and assessed with automated processes, be integrated in intelligent applications, and to provide an interoperable semantic-based solution to certify ROPA legal compliance.

4.3.2 SOFTWARE INTEROPERABILITY

Heavy use of **standards** will guarantee interoperability. This is a data-driven design. Software interoperability will benefit from the use of standards for the data each module exchanges inside the OntoROPA ecosystem and with other blocks of ONTOCHAIN. The eIDAS Regulation (Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market) sets a framework for electronic identification and trust services for electronic transactions in the European single market. Compliance with this Regulation will guarantee interoperability in interactions with identity services. The X.509 standard will be used for digital certificates. As for the rest of data, reference to RDF standard and other related W3C standards has been presented in this section. Smart contracts will provide interoperability with other Ontochain members.

4.4 IMPLEMENTATION PLAN

4.4.1 Methodology for software specifications

The proof of concept of *OntoROPA* for First ONTOCHAIN Call is focused on the use case presented in this document: publication of ROPAs. The community interested is ROPA controllers (ROPA providers). Communities will be managed in the following phases. For each module in the architecture presented in Figure 3, there is a proof of concept. Table 8 reminds the work plan for the three years project and Table 9 the work

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

plan for First ONTOCHAIN Call. Finally, Table 10 details the work plan for the next phase of First Call: Proof of Concept.

Work package	Description	Starting Month	Ending Month
WP1: *OntoROPA* proposal	First version of the *OntoROPA* ontological ecosystem. Proof of concept.	Month 1	Month 7
WP2: *OntoROPA* Community	Collaborative refinement of *OntoROPA* with the community of public sector ROPA controllers.	Month 7	Month 19
WP3: Application to real ROPAs	Use of *OntoROPA* with the ROPAs controlled by the community involved in WP2	Month 20	Month 34

Table 8. Work plan for three years project

Work plan task	Description	Starting Month	Ending Month
WT1: Research proposal	Design of the architectural framework (software, data and knowledge, legal) that will support the *OntoROPA* ecosystem.	Month 1	Month 2
WT2: Design and proof of concept	Design of the 1st version of the *OntoROPA* framework. Proof of concept with a set of ROPAs obtained from public administration.	Month 3	Month 6
WT3: Publication	Preparation of a publication with the results from WT1 (Phase 1) and WT2 (Phase 2).	Month 3	Month 7

Table 9. Work plan for 7 months (First ONTOCHAIN Call)

Work plan task	Description	Starting Month	Ending Month
WT2.1: Knowledge Acquisition	First iteration of expert knowledge acquisition (competency questions) and initial ontology design.	Month 3	Month 5
WT2.2: Linked ROPAs	Proof of concept for Linked ROPAs module	Month 3	Month 4
WT2.3: Proactiveness & Certification	Proof of concept for Proactiveness and Certification modules	Month 4	Month 5
WT2.4: OntoROPA Ontology v1.0	First validated draft of the OntoROPA Ontology	Month 4	Month 6
WT2.5: Identity	Proof of concept for Identity module	Month 5	Month 6
WT2.6: Validation	Proof of concept for Validation module	Month 5	Month 6

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Table 10. Work plan for Proof of Concept (First ONTOCHAIN Call)

WT2: Design and proof of concept	M 1	M 2	M 3	M 4	M 5	M 6	M 7
WT2.1: Knowledge Acquisition			■	■	■		
WT2.2: Linked ROPAs			■	■			
WT2.3: Proactiveness & Certification				■	■		
WT2.4: OntoROPA Ontology v1.0				■	■	■	
WT2.5: Identity					■	■	
WT2.6: Validation					■	■	

Table 11. Work plan TIMELINE (First ONTOCHAIN Call)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

5 CONCLUSIONS

The design presented contains the proof of concept we can develop in 4 months, which is the real time left from now until the end of Phase 2. It covers the use case we called *New ROPA*. ROPA stands for 'Records of Processing Activities' (according to Recital 82 and Art. 30 of GDPR). ROPA providers will be able: (i) to create a new ROPA, (ii) use OntoROPA facilities to reach legal validity and to add legal value, (iii) and to publish it (also according to GDPR requirements to enhance citizens' and consumers' rights).

Thus, this is a *smart* new ROPA, as (i) it provides technical innovative solutions, (ii) automates the required legal procedural requirements with Compliance by Design and Through Design (CbD/CtD), (iii) and creates social and economic value. The overall design refers to a new LawTech Web Service, located on ONTOCHAIN, and able to generate a complete legal ecosystem, decentralised and distributed among several communities (providers). Doing so, it solves the blockchain issues and concerns about GDPR compliance raised by EU privacy experts and several national and international institutions.

The OntoROPA team has advanced in the architecture design, covering both data and software within three different dimensions (technological, social, and legal). The modular software architecture facilitates the organization of independent proofs of concept for each layer. The clean separation of software and data facilitates an independent ontology building process, with its own specific methodology, workflows, tasks, and milestones.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

REFERENCES

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, 54(2), 442–492.

Blomqvist, E. (2004). *State of the Art: Patterns in Ontology Engineering. Technical Report 04:8*. Jönköping University.

Boella, G., Tosatto,S.C., Ghanavati, S., Hulstijn, J.,Humphreys, L.,Muthuri, R., Rifaut, A., & van der Torre, L.(2013). Integrating legal–urn and eunomos: Towards a comprehensive compliance management solution. In *International Workshop on AI Approaches to the Complexity of Legal Systems* (pp. 130–144). Springer.

Casanovas, P., Hashmi, M., Lam, B., & de Koker, G. (2021). Legal Compliance by Design (LCbD) and through Design (LCtD): A Literature Survey (forthcoming).

Casanovas,P. (2021). "Inteligencia Artificial y Derecho: La doble implosión de las profesiones y servicios jurídicos en la era digital" [Artificial Intelligence and Law: The Double Implosion of Legal Professions and Services in the Digital Age]. In: Velarde, Olivia & Martín, Manuel (Eds.) 2021. Mirando hacia el futuro. Cambios sociohistóricos vinculados a la virtualización. Madrid: Centro de Investigaciones Sociológicas (CIS) [Ministerio de la Presidencia]. In Press.

CNIL (2018). *Blockchain. Solutions for a responsible use of the blockchain in the context of personal data.* https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

Davies, J., Welch, J., Milward, D., & Harris, S. (2020). A formal, scalable approach to semantic interoperability. Science of Computer Programming. 192. https://doi.org/10.1016/j.scico.2020.102426

Doran, P. (2006). Ontology Reuse via Ontology Modularisation. In *Proceedings of KnowledgeWeb PhD, Symposium 2006 (KWEPSY2006)*. Budva.

Fernández-López, M., Gómez-Perez, A., & Juristo, N. (1997). Methontology: from ontological art towards ontological engineering. In Farquhar, A. & Gruninger, M. (Eds.), *Ontological Engineering: Papers from the 1997 Spring Symposium AAAI97, volume Technical Report SS-97-06* (pp. 33-40). American Association for Artificial Intelligence.

Fink, M.(2019)*Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?* EPRS, European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Governatori, G., Barnes, J., Zeleznikow, J. Hashmi, M., de Koker, L.,Poblet, M., & Casanovas, P. (2020). `Rules as Code' will let computers apply laws and regulations.But over-rigid interpretations would undermine our freedoms. *The Conversation*, 26 November 2020, https://theconversation.com/rules-as-code-will-let-computers-apply-laws-and-regulations-but-over-rigid-interpretations-would-undermine-our-freedoms-149992

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

Humphreys, L., Boella, G., van der Torre, L., Robaldo, L., Di Caro,L., Ghanavati, S., & Muthuri, R. (2020). Populating legal ontologies using semantic role labeling. *Artificial Intelligence and Law*, 1–41.

Pagallo, U., Casanovas, P., & Madelin, R. (2019). The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data. *The Theory and Practice of Legislation*, 7(1),1–25.

Poblet, M., Casanovas, P., Rodríguez-Doncel, V. (2019). Linked Democracy. Foundations, methodology and applications. Springer Brief in Law n. 750. Open Access. https://link.springer.com/book/10.1007/978-3-030-13363-4

Waddington, M. (2020). Research Note. Rules as Code. *Law in Context*, 37(1), 1–8. https://doi.org/10.26826/law-in-context.v37i1.134

Wyner, A.Z., & Governatori, G. (2013). A Study on Translating Regulatory Rules from Natural Language to Defeasible Logics. In *RuleML* (2).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338

APPENDIX A

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957338