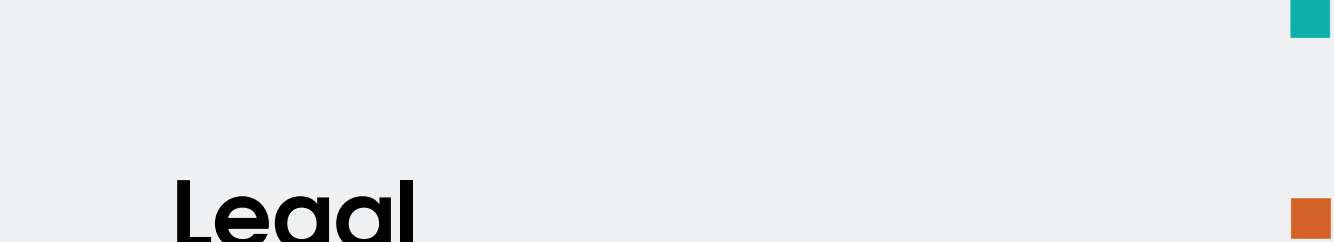
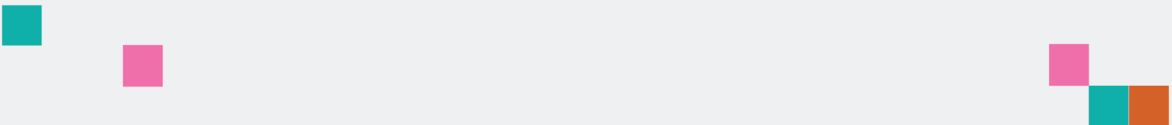
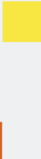




decode



**Legal
frameworks for
digital commons
DECODE OS and
legal guidelines**



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 732546



Project no. 732546

DECODE

DEcentralised Citizens Owned Data Ecosystem

D1.8 Legal Framework for digital commons DECODE OS Legal Guidelines

Version Number: V1

Lead beneficiary: Politecnico di Torino (POLITO)

Due Date: October 2017

Author(s): Eleonora Bassi (Politecnico di Torino), Marco Ciurcina (Politecnico di Torino), Juan Carlos De Martin (Politecnico di Torino), Selina Fenoglio (Politecnico di Torino), Giulia Rocchi (CNRS), Oleguer Sagarra Pascua, Francesca Brial (IMI)

Editors and reviewers: Ricard Espelt (UOC-Dimmons), Stefano Lucarelli (CNRS), Denis Rojo (Dyne)

Dissemination level:		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

**Approved by: Francesca Bria (Chief Technology and Digital Innovation Officer
Barcelona City Hall)**

Date: 31/10/2017

This report is currently awaiting approval from the EC and cannot be not considered to be a final version.

Executive summary

This document reviews the legal frameworks that may hamper the building of digital commons (from free software to data) including the case in which such digital commons concern the use of personal data.

From the analysis of the technical features of the DECODE technology, practical guidelines for the design of the DECODE OS and the DECODE smart rules syntax will follow as a result.

In the first section we examine the different legal frameworks involved in the use of the DECODE technology in view of fostering the creation of digital commons (see below Annex A).

We examine the relevant and applicable legislations, which depend on the territorial context, and the legal tools emerged in the last decades, particularly in the copyright and patent legal domain.

The subsections of this part of the document aim to analyse different legal domains: copyright and intellectual property rights, data protection and other legal fields related to data sharing.

In section 2 we analyse how to lawfully set the DECODE technology. In light of current and established tools, such as free licenses, we explore the opportunities offered by the DECODE technology in order to write and adopt smart rules.

Next, focus is on how the DECODE technology allows the processing of personal data in compliance with the EU privacy rules (GDPR, etc.).

On the one hand, we adopt the precautionary rule of taking into consideration already existing feasible solutions even for the worst possible scenario. On the other hand, new legal tools and strategies are defined in accordance with a proactive approach.

Finally, section 3 aims to provide practical support to the technical work to be performed within the DECODE Project. The legal analysis conducted throughout this document will provide a list of recommendations.

The document includes three Annexes. Annex A offers an overview of the debate on the definition of 'digital commons'. Annex B is a legal taxonomy that supports the design of the ontologies to be adopted within the project for the implementation of the DECODE technology: it also provides the conceptual tools necessary to understand the key notions of the different legal domains. Annex C is a legal bibliography relevant for the DECODE Project.

This document was written with the contribution of Priya Samuel (TW) and Pau Balcells Alegre (IMI).

Contents

Introduction	5
Acronyms Table	6
1. Legal frameworks	7
1.1 Applicable law	7
1.2 Intellectual property rights.....	10
1.2.1 EU legal framework & highlights	11
1.2.1.1 Copyright and related rights	11
1.2.1.2 Copyright and sui generis right on databases	14
1.2.1.3 Patents and other industrial rights.....	16
1.2.2 Free licenses	21
1.2.2.1 Free licenses history	22
1.2.2.2 Free licenses characteristics.....	30
1.2.2.3 Free software licenses: some considerations for the DECODE project	31
1.2.3 Distributed ledgers architectures and intellectual property rights	34
1.3 Privacy and data protection law	35
1.3.1 EU legal framework & highlights	35
1.3.1.1 The notion of personal data	35
1.3.1.2 General principles and definitions on personal data processing.....	37
1.3.1.3 Data subject’s rights	39
1.3.1.4 The control of the data processing, obligations and responsibilities	44
1.3.2 Distributed Ledgers Architectures & privacy issues to be faced	48
1.4 Other limitations to data sharing and reuse	50
1.4.1 Rights of the personality and other rights.....	50
1.4.2 Statistical confidentiality and public security secrecy	51
2. Strategies, Measures, Technical Tools.....	53
2.1 Different solutions for different ownerships	53
2.2 Smart rules and smart contracts.....	55
2.3 Free licenses for DECODE.....	58
2.3.1 Free licenses for the DECODE technology.....	58
2.3.2 Free licenses for the data shared with DECODE.....	60
2.4 Legal rules and technical strategies for privacy and data protection compliance	60
2.4.1 Legal rules and technical strategies for privacy and data protection compliance of DECODE OS	61
2.4.2 Legal rules and technical strategies for privacy and data protection compliance of data processing within services based on DECODE technology	62
3. Legal guidelines for the development of the DECODE OS.....	65
3.1 Recommendations	65

3.1.1	Recommendations on the design of DECODE OS	65
3.1.2	Recommendations on the design of smart rules syntax.....	66
3.2	Legal domain taxonomy	67
4.	References.....	68
Annex A:	Notes for a definition of Digital Commons.....	71
1.	Digital commons definition.....	71
1.1	From knowledge commons to digital commons. The Ostromian perspective and beyond.....	72
1.2	New digital rights for a new technological paradigm: the digital commons in the perspective of the free software movement	77
1.3	Towards a practical definition of Digital Commons.....	78
1.4	References.....	80
Annex B:	Taxonomy	82
Annex C:	Bibliography	88
1.	Digital Commons.....	88
2.	Legal aspects of Blockchain and Distributed Decentralized Architectures.....	89
3.	IPRs & Licensing	91
3.1	IPRs & Blockchain.....	93
3.2	Legislation	93
3.2.1	EU legislation.....	93
3.2.2	International Treaties	95
3.3	Opinions, recommendations and standards	96
4.	Privacy and data protection	96
4.1	Privacy & Blockchain.....	98
4.2	Legislation	99
4.3	Recommendations and standards.....	99
5.	Smart Contracts	100

Introduction

The aim of the document is to provide an overview of the legal rules to be applied within the DECODE Project, and to examine what strategies may follow.

Those rules and strategies allow the fulfillment of the objectives of the Project, including the ethical ones, by addressing some of its challenges, such as the creation of “a framework in which people want to share their data in a controlled way for the common good” and the identification of “the right way to manage decentralized digital platforms so that contributors have a genuine stake and say in how they run”¹.

The ethical issues concern both the creation of digital commons and the management of digital data as commons, e.g. freedom of expression, transparency, data sovereignty, and openness. Although these issues will arise in the practical use (e.g. within the Pilots) of DECODE OS, according to the legal rules that allow and enforce it, such issues are not considered in this document.

In the first section we examine the different legal frameworks involved by the use of the DECODE technology. The objective is to provide a clear vision of the binding rules that must be taken into account for the development of the project, as minimum mandatory standard requirements. Accordingly, we scrutinize the relevant and applicable legislations, which depend on the territorial context, and the legal tools emerged in the last decades, particularly in the copyright and patent legal domain. The subsections of this part of the document aim to analyse different legal domains: copyright and intellectual property rights, data protection and other legal fields related to data sharing.

In section 2 we analyse strategies and legal tools so as to lawfully set the DECODE technology, in a way that fosters the creation and trusty diffusion of digital data commons².

Finally, legal guidelines and a list of recommendations for the development of DECODE OS are provided. Those recommendations concern, for example, the use of licenses, smart rules embedding contracts or other legal acts binding for the contractors, disclaimers, and legal statements for managing (personal) data sharing.

¹ See T. Symons, T. Bass (2017), Project methodology and policy review.

² See T. Symons, T. Bass (2017), Project methodology and policy review, that mentions the necessity of legal tools for “Giving people privacy-preserving mechanisms for interacting with online services (...); Supporting the development of platform cooperativism (...); Enabling data to be used for social good through the creation of a family of data commons. This could include a combination of personal data, city open data and private data”.

Acronyms Table

Acronym	Meaning
CC	Creative Commons
CC0	Creative Commons 0 – Public Domain Dedication
CC-BY	Creative Commons Attribution
DECODE OS	Decode Operating System
DLD	Distriduted Ledgers Developer (who develops and licenses the software that allows the DLT to run)
DLS	Distriduted Ledgers Storer (who runs the software that allows the DLT to run and stores the DLT)
DLSC	Distriduted Ledgers Service Controller (entity who determines the objectives and the purposes of a service and the adoption of DLT and SR for its realization)
DLT	Distributed Ledgers Technology
DPO	Data Protection Officer
EUPL	European Union Public License
GDPR	General Data Protection Regulation
GNU-AGPL	GNU Affero General Public License
GNU-GPL	GNU General Public License
GNU	GNU's Not Unix
LGPL	<i>GNU</i> Lesser General Public License
PIA	Privacy Impact Assessment
SR	Smart Rule
SRC	Smart Rule Creator (who publishes on the DLT a SR (model) that can be used by different parties but he is not a SRDP, SRDR, or DLSC)
SRDP	Smart Rule Data Provider (SR party that provides his personal data)
SRDR	Smart Rule Data Recipient (SR party that gets access to personal data to use it (becoming data controller)

1. Legal frameworks

In the following sections we examine the different legal frameworks that should be taken into account within the DECODE Project. Particular attention will be drawn to the goal of fostering the building of digital commons as defined within the project (see **Annex A**).

Section 1.1 examines the relevant and applicable legislations and domains, depending on the territorial context, the entities involved and the main characteristics of the services and processing.

Next we analyze the copyright and intellectual property rights framework (1.2); then, the data protection legislation (1.3); and, finally, some other limitations to data sharing (1.4).

1.1 Applicable law

DECODE is an Horizon 2020 project funded by the European Union that aims to design and release a technology to be initially used in Europe by the pilots to be developed within the project.

However, the territory this document will go through is not stable and solid but is a land of continuous changes and interventions by legislators and courts. Moreover, the uncertainty of this new context is a challenge for lawmakers that explore new tools and strategies to exploit distributed ledger technologies (DLT), in light of the different principles and fundamental rights enshrined in the European Treaties and constitutions of the Member States³.

Some of the relevant fundamental rights and principles that concern the use of the DECODE technology, based on DLT and smart rules (SR), are mentioned by the

³ See European Parliament Resolution of 26 May 2016 on virtual currencies (2016/2007(INI)), Article 9 that: *“Recognises the still unfolding potential of DLT well beyond the financial sector, including crypto-equity crowdfunding, dispute mediation services, in particular in the financial and juridical sectors, and the potential of smart contracts combined with digital signatures, applications allowing for heightened data security and synergies with the development of the Internet of Things”*.

European Parliament Resolution of 26 May 2016 on virtual currencies⁴. For example, Article 8 of this Resolution mentions transparency and trustworthiness: “*DLT could be used to increase data sharing, transparency and trust not only between government and citizens, but also between private sector actors and clients*”.

How to strike a fair balance between data sharing and trust, freedom of information and freedom of expression, open democracy and digital sovereignty, privacy awareness and transparency, remains of course an open issue. For instance, the potential transparency of transactions through DLT may imply risks of surveillance. Moreover, although cryptography, which is one of the core aspects of DECODE technology, may strengthen privacy and the protection of personal data⁵, it should be admitted that anonymity can raise issues of accountability, and so forth⁶. The challenges addressed by the DECODE Project concern the design of technical and legal tools for managing this complex scenario so as to abide by the European law and the general principles of law applicable in Member States.

Compliance with each and all the laws applicable in the Members States has to be further evaluated in connection with specific use cases, including the pilots: as a matter of fact, it should always be clear to adopters of the technology that laws apply in a territorial context.

National laws are thus the context to be considered, even when the Member States shall apply the European legislation.

Two of the most relevant legislative frameworks that concern the DECODE technology illustrate how to grasp the dynamics between National States and EU law, namely:

- a) copyright and related rights, including sui generis rights on databases;
- b) privacy law and personal data protection legislation.

Concerning copyright and related rights, as it will be further illustrated in the following sections 1.2.1.1 and 1.2.1.2, the European legislation and the applicable international

⁴ European Parliament Resolution of 26 May 2016 on virtual currencies (2016/2007(INI)), <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2016-0228>.

⁵ See for example the analysis made by Primavera De Filippi on the relation between transparency, confidentiality and data sovereignty: P. De Filippi (2016). The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies. *Journal of Peer Production*, Issue n.7: Alternative Internets. Available at SSRN: <https://ssrn.com/abstract=2852689>. See also R. Peeters, and T. Pulls (2015). *Regaining the end-users' trust with transparency-enhancing tools*. In Amsterdam Privacy Conference 2015.

⁶ The European Parliament alerts on this crucial issue: “*DLT have the potential to contribute positively to citizens' welfare and economic development, including in the financial sector, by means of: (d) enabling systems that combine ease of use, low transaction and operational costs and a high degree of privacy, but without full anonymity so that transactions are traceable to a certain extent in case of malfeasance and so that transparency for market participants in general can be increased*”, Article 1, point d, European Parliament resolution of 26 May 2016 on virtual currencies (2016/2007(INI)).

treaties permit to assume a fairly high degree of uniformity within the different Member States (and, to a minor extent, considering international treaties, also to other states).

Concerning privacy, it's important to highlight that the GDPR applies widely, including to entities not based in EU, according to Articles 2 and 3 of the GDPR.

The GDPR, Article 2(1) provides the following:

"This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system".

Article 3 on "Territorial scope" provides the following:

"(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- 1.the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
- 2.the monitoring of their behaviour as far as their behaviour takes place within the Union.*

(3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law".

It is worth mentioning that, in this field, the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') should apply⁷.

Particularly, Article 14 (Hosting), that provides that a service provider should not be responsible as long as *"does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent"* and, *"upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information"*.

This applies both in respect of copyright and related rights violations, but also in respect of privacy violations.

Concerning privacy, GDPR, Article 2(4) states:

⁷ See <http://data.europa.eu/eli/dir/2000/31/oj>

“This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive”.

Moreover, the Recital 21 of the GDPR states:

“This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States”.

1.2 Intellectual property rights

Intellectual property is an expression used to refer to: copyright and related rights, trademarks, geographical indications, industrial designs, patents, plant varieties, layout-designs of integrated circuits, and trade secrets.

Intellectual property rights, usually, are regulated at national level: they are normally acquired and enforced on a country-by-country basis, and rules applying and exceptions and limitations vary from one state to another.

But IPRs, that apply to immaterial goods, move easily through borders. This is why the need of regulating intellectual property rights at the international level was identified as a goal to achieve since the XIX century and, nowadays, there are many international treaties that regulate the different IPRs.

Particularly relevant (because of its wide spectrum of rights regulated) is the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS).

The TRIPS Agreement was signed in 1994; it is administered by the WTO and applies to all member states of the same WTO: nowadays it is a strong driver towards standardization of IPRs at international level.

As a matter of fact, the expression ‘intellectual property’ refers to different rights, that operate according to different rules that have different effects and purposes.

The use of the term is discussed within the free software community. Richard Stallman, founder of the GNU project, suggests to avoid the use of the expression: it is confusing (because it mixes different things) and it is misleading (because induces the wrong perception that it works like property of material goods)⁸.

⁸ See <https://www.gnu.org/philosophy/not-ipr.en.html>.

Actually, assigning exclusive rights to the owners of material goods, proved to be an effective strategy through centuries: it is an almost implicit knowledge of most people with standard western culture that property “is good”. But over the past decades, since the raise of the internet, a growing number of people deem that exclusive rights for immaterial goods are not as good as they are for material goods. Property does not only hinder sharing but, as a result, can damage society.

In this ethical conflict, practices fostering sharing and reuse of digital goods emerged as a way to tackle the inefficiency of the so-called intellectual property rights.

Some of the so-called intellectual property rights interfere with implementation and use of the DECODE technology.

On the one hand, some rights (particularly copyright on software and patents) could interfere with the implementation of the technology and its sharing.

On the other hand, some rights (particularly copyright and sui generis rights on databases) could interfere with the use of the technology that, in its essence, allows creation and sharing of datasets (that could be subject to such rights).

A digital commons-triggering technology requires to take into account such legal schemes, as the licences, with which to identify the proper techniques and practices to be adopted to bypass the problem of IPRs. The latter can indeed hinder the use and sharing of the DECODE technology.

1.2.1 EU legal framework & highlights

This section focuses on the EU legal frameworks regulating IPRs that can interfere with the implementation and use of the DECODE technology.

In the subsections the different relevant legal tools and the EU rules that apply for each of them are briefly described.

1.2.1.1 Copyright and related rights

Copyright and related rights are regulated at international level by the TRIPS Agreement and a number of other international treaties, including:

- Berne Convention for the Protection of Literary and Artistic Works:

Signed in 1886, it is the oldest and most important treaty about copyright. It establishes minimum standards of protection, the types of works protected, duration of protection, scope of exceptions and limitations, besides principles such as “national treatment” (works originating in one signatory country are

given the same protection in the other signatory countries as each country grants to works of its own nationals), and “automatic protection” (copyright inheres automatically in a qualifying work upon its fixation in a tangible medium and without any required prior formality).

- Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations:

It was signed in 1961 and regulates protection of performances, phonograms and broadcasting.

- WIPO Copyright Treaty (WCT) and WIPO Performers and Phonograms Treaty (WPPT):

They were signed in 1996. WCT provides that software and databases are protected by copyright. The two treaties recognize that the transmission over the Internet and similar networks is protected by an exclusive right, and define as infringements both the circumvention of technological protection measures, and the removal of embedded rights management information.

The following directives regulate copyright and related rights within the European Union:

- Directive 93/83/EEC (“Satellite and Cable Directive”)⁹;
- Directive 96/9/EC (“Database Directive”)¹⁰;
- Directive 2001/29/EC (“InfoSoc Directive”)¹¹;
- Directive 2001/84/EC (“Resale Right Directive”)¹²;
- Directive 2004/48/EC (“IPRED”)¹³;
- Directive 2006/115/EC (“Rental and Lending Directive”)¹⁴;
- Directive 2006/116/EC¹⁵ and Directive 2011/77/EU¹⁶ (“Term Directives”);

⁹ Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission; see <http://data.europa.eu/eli/dir/1993/83/oj>.

¹⁰ Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases; see <http://data.europa.eu/eli/dir/1996/9/oj>.

¹¹ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; see <http://data.europa.eu/eli/dir/2001/29/oj>.

¹² Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art (“Resale Right Directive”); see <http://data.europa.eu/eli/dir/2001/84/oj>.

¹³ Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights; see <http://data.europa.eu/eli/dir/2004/48/corrigendum/2004-06-02/oj>.

¹⁴ Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property; see <http://data.europa.eu/eli/dir/2006/115/oj>.

- Directive 2009/24/EC (“Software Directive”)¹⁷;
- Directive 2012/28/EU (“Orphan Works Directive”)¹⁸;
- Directive 2014/26/EU (“CRM Directive”)¹⁹.

Copyright gives the creator of an original work exclusive rights to use it for a certain period of time.

Rights conferred by copyright laws include ‘the right to copy’, but also the right to be credited for the work, to determine who may adapt the work to other forms, who may perform the work, who may distribute it, etc.

Copyright applies to expressible forms of ideas or information but does not protect the idea or information itself: this means that, for copyright to be infringed, one has to copy the form in which the ideas or information are expressed.

The Berne Convention (Article 2) provides that, at a minimum, copyright protection in all signatory countries should extend to “*literary and artistic works*”, including “*every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression*”.

The detailed list of categories of works that are protected by copyright – and the specific definition and scope of each of them – may slightly vary from country to country, but it generally includes scientific articles, essays, novels, short stories, poems, plays and other literary works, drawings, paintings, photographs, sculptures and other two and three dimensional pieces of art, films and other audiovisual works, and musical compositions.

In the last decades copyright has been applied to software and databases as a result of case law decisions in different states and legislative choices adopted²⁰, even at an international level²¹.

¹⁵ Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights; see <http://data.europa.eu/eli/dir/2006/116/oj>.

¹⁶ Directive 2011/77/EU of the European Parliament and of the Council of 27 September 2011 amending Directive 2006/116/EC on the term of protection of copyright and certain related rights; see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:265:0001:0005:EN:PDF>.

¹⁷ Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs; see <http://data.europa.eu/eli/dir/2009/24/oj>.

¹⁸ Directive 2012/28/EU of the European Parliament and of the Council of 25 October 2012 on certain permitted uses of orphan works; see <http://data.europa.eu/eli/dir/2012/28/oj>.

¹⁹ Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market; see <http://data.europa.eu/eli/dir/2014/26/oj>.

²⁰ In the European Union was adopted the Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, repealed by the Software Directive, see note 15.

²¹ Among others, see Article 10 of the TRIPS Agreement.

Related rights are, among others, the right of performers, phonogram producers, broadcasting organisations, and film producers: they are rights that relate to copyright but, usually, are conferred to third parties making use (with due authorization) of the works covered by copyright.

According to the Berne Convention, the author is “*the creator of an artistic work*” (Article 2); often copyright is shared by multiple authors.

Some national legislations provide for automatic assignment of some rights of the author to a third party according to specific circumstances (such as, the assignment of the economic rights of a worker to the subject he works for).

Copyrights can be separated in two groups, with different characteristics:

- Moral rights:

their regime differs greatly between countries, but typically includes the right to be identified as the author of the work (right of paternity or right of attribution) and the right to object to any distortion or mutilation of the work (right of integrity) which would be prejudicial to the honour or reputation of the author. (Berne Convention, art. 6bis);

- Economic rights:

the major economic rights consist of the exclusive right of the authors to authorize reproduction, performance, broadcasting, public recitation, translation, adaptation, arrangements, alterations, creation and performance of cinematic adaptations (Berne Convention, Articles 8, 9, 11, 11bis, 11ter, 12, and 14).

According to Article 1(1) of the Term Directives the right of the author “*shall run for the life of the author and for 70 years after his death*” and the right of performers and phonogram producers can run for 70 years.

Copyright and related rights are subject to limitations that vary from country to country.

1.2.1.2 Copyright and sui generis right on databases

The Database Directive provides for two different sets of property rights that apply to databases: copyright and the *sui generis* right on database²².

Database is defined by Article 1(2) as “*a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means*”.

²² Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

It is important to stress that copyright and the *sui generis* right on databases do not apply to data that are not arranged in a database.

According to Article 3(1) “databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright”, and, according to Article 3(2) copyright protection of databases “shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves”.

The copyright owner of the database is “the natural person or group of natural persons who created the base or, where the legislation of the Member States so permits, the legal person designated as the rightholder by that legislation” (Article 4(1)).

According to Article 5 of the Database Directive the author of a database protected by copyright “shall have the exclusive right to carry out or to authorize:

(a) temporary or permanent reproduction by any means and in any form, in whole or in part;

(b) translation, adaptation, arrangement and any other alteration;

(c) any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the right-holder or with his consent shall exhaust the right to control resale of that copy within the Community;

(d) any communication, display or performance to the public;

(e) any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b)”.

The Term Directives regulate duration of copyright, including copyright on databases that, therefore, “shall run for the life of the author and for 70 years after his death”.

Some exceptions to the above mentioned restricted acts are provided by Article 6.

Even though copyright does not apply to a database, it could be protected by the *sui generis* right provided by Articles 7-11: according to Article 7(4) “The right provided for in paragraph 1 shall apply irrespective of the eligibility of that database for protection by copyright or by other rights”.

Article 7(1) of the Database Directive provides that “the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents” has the right “to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database”.

According to Article 7(2):

“For the purposes of this Chapter:

(a) 'extraction' shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form;

(b) 're-utilization' shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the right-holder or with his consent shall exhaust the right to control resale of that copy within the Community;

Public lending is not an act of extraction or re-utilization".

It is worth mentioning that according to Article 8:

"1. The maker of a database which is made available to the public in whatever manner may not prevent a lawful user of the database from extracting and/or re-utilizing insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. Where the lawful user is authorized to extract and/or re-utilize only part of the database, this paragraph shall apply only to that part.

2. A lawful user of a database which is made available to the public in whatever manner may not perform acts which conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database".

Also, according to Article 7(5) *"The repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database shall not be permitted".*

According to Article 10, the *sui generis* right on a database expires after 15 years from its completion or making available to the public and the term starts again if the database is subject to substantial changes.

Article 9 provides for some exceptions to the restricted acts provided by Article 7.

Finally, Article 11 limits the applicability of the *sui generis* database rights to nationals of (or resident in) a member state and to European companies.

For the *sui generis* right on databases to become operative (like for copyright) no registration is required.

1.2.1.3 Patents and other industrial rights

Other so called IPRs could be relevant for the DECODE technology deployment and use.

This section sums up some details about such rights: (a) patents, (b) trademarks, (c) layout design of integrated circuits, (d) industrial design, (e) trade secrets, and (f) other IPRs.

a) Patents

Patent is the set of rights that national States award to the person or entity that applies for protection of an invention that is new, involves an inventive step, and is capable of industrial application.

The patent is awarded for a limited period of time (usually 20 years since the deposit of the application).

Rights conferred to the applicant usually consist in the right to exclude third parties from making, using, selling, offering for sale, or importing the patented invention.

The European legislation does not provide harmonization rules on the patent subject matter.

Nevertheless, patent law in Europe is fairly homogeneous because member states participate to different international treaties that regulate patents, including the patent subject matter.

The TRIPS Agreement regulates patents at Articles 27-34.

Other relevant international treaties are the following:

- the Patent Cooperation Treaty (PCT) signed in 1970 that provides a unified procedure for filing patent applications in member states;
- the Convention on the Grant of European Patents of 5 October 1973 (European Patent Convention or EPC) that provides for substantial rules on the subject matter and a unified procedure for filing patents in multiple member states.

At the European Union level, an effort to achieve further uniformity in patent legislation led to the approval in December 2012 by the EU Parliament and Council of the so called “*EU patent package*”, consisting of two EU regulations and an intergovernmental treaty:

- Regulation 1257/2012²³,
- Regulation 1260/2012²⁴,
- Agreement on a Unified Patent Court (UPC)²⁵, EU Document 16351/12.

²³ Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection; see <http://data.europa.eu/eli/reg/2012/1257/oj>

²⁴ Council Regulation (EU) No 1260/2012 of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection with regard to the applicable translation arrangements; see <http://data.europa.eu/eli/reg/2012/1260/oj>

The UPC Agreement is still not applicable; it will enter into force after some conditions will be met.

The Regulations will apply to all participating States from the moment the UPC Agreement will enter into force.

The EU adopted some other legal acts that refer to specific aspects of the patent law (e.g. the Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the patentability of biotechnological inventions) but they do not have relevance for the DECODE Technology.

The issue of software patentability is particularly relevant for DECODE technology. Although the substantial rules governing patent subject matter are very similar in the different Member States, judges of the different States adopted different rulings about the patentability of software.

Adopting software that interferes with patented inventions could affect users of specific countries of some European countries (and other extra UE countries). Therefore, avoiding the use of patented technologies is a goal to achieve for the DECODE technology.

b) Trademarks

A trademark is a sign capable of distinguishing the goods or services of one enterprise from those of other enterprises.

Trademark right allows the owner of the right to use the trademark, including licensing it to third parties.

Trademarks can be registered, thus receiving stronger protection, and the registered trademark right lasts until the owner continues to pay the due registration fees.

The European Union regulates trademarks with different legal acts:

- Directive 2008/95/EC²⁶ (which, according to Article 65 of the Directive (EU) 2015/2436, is repealed with effect from 15 January 2019);
- Directive (EU) 2015/2436²⁷;
- Regulation (EU) 2017/1001²⁸.

²⁵ Agreement on a Unified Patent Court (UPC), EU Document 16351/12; see <https://www.unified-patent-court.org/sites/default/files/upc-agreement.pdf>

²⁶ Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trademarks; see <http://data.europa.eu/eli/dir/2008/95/oj>

²⁷ Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trademarks; see <http://data.europa.eu/eli/dir/2015/2436/oj>

²⁸ Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark; see <http://data.europa.eu/eli/reg/2017/1001/oj>

Directive 2008/95/EC and Directive 2015/2436/EU provide for harmonization of trademark national laws regulating trademarks (and their registration) at national level.

Regulation 2017/1001 provides for the possibility to register unitary trademarks, that is trademarks that have a unitary effect all over the European Union.

c) Layout-design of integrated circuits

Layout-design of integrated circuits, topography of semiconductor products, and mask design, are three different names for the same right protected in different countries around the world and integrated into the TRIPS Agreement pursuant to Article 35.

The European Union regulates layout-designs of integrated circuits with the Directive 87/54/EEC²⁹.

Article 1 of the Directive 87/54/EEC provides the following definitions:

“(a) a ‘semiconductor product’ shall mean the final or an intermediate form of any product:

(i) consisting of a body of material which includes a layer of semiconducting material; and

(ii) having one or more other layers composed of conducting, insulating or semiconducting material, the layers being arranged in accordance with a predetermined three-dimensional pattern; and

(iii) intended to perform, exclusively or together with other functions, an electronic function;

(b) ‘topography’ of a semiconductor product shall mean a series of related images, however fixed or encoded;

(i) representing the three-dimensional pattern of the layers of which a semiconductor product is composed; and

(ii) in which series, each image has the pattern or part of the pattern of a surface of the semiconductor product at any stage of its manufacture”.

The Directive 87/54/EEC provides for an exclusive right to commercially use the topography for 10 years to the natural person that created the topography or to the company he works for.

Article 4 of the Directive 87/54/EEC provides that members states could require registration for the right to be awarded.

²⁹ Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products; see <http://data.europa.eu/eli/dir/1987/54/oj>

This right could interfere with the design of semiconductors eventually adopted to implement the DECODE technology and/or designed within the project for the same purpose.

d) Industrial design

Industrial design is the ornamental or aesthetic aspect (not being merely functional) of an item. It may consist of three dimensional features (such as the shape of an artefact) or two dimensional features (such as patterns, lines or color).

As occurs with trademarks, in the European Union legal protection of industrial design coexists with EU legal protection coexist..

Directive 98/71/EC provides for harmonised standards for eligibility and protection of industrial design³⁰.

Regulation (EC) No 6/2002 provides a unitary right protecting registered community design for up to 25 years (but also, for three years, for unregistered design)³¹.

Industrial design should not interfere with the implementation of the DECODE technology but this cannot be completely excluded.

e) Trade secrets

A trade secret is a valuable and confidential piece of information for an enterprise that gives that enterprise a competitive advantage.

Trade secrets are protected without any procedural formalities, that is, there is no need for registration.

Consequently, a trade secret can be protected for an unlimited period of time.

The TRIPS Agreement regulates undisclosed information (or trade secrets or know-how) in Article 39.

Even though the TRIPS Agreement does not expressly require undisclosed information to be awarded a property right, it states that "*Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices*".

In EU trade secrets are regulated by the Directive (EU) 2016/943 ("Trade Secrets Directive")³².

³⁰ Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs; see <http://data.europa.eu/eli/dir/1998/71/oj>

³¹ Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs; see <http://data.europa.eu/eli/reg/2002/6/2013-07-01>

Article 2(1) of the Trade Secrets Directive defines trade secret as “*information which meets all of the following requirements:*

(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) it has commercial value because it is secret;

(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret”.

The Trade Secrets Directive provides for protection from unlawful conduct by which someone acquires or discloses, without authorisation and through illicit means, information with commercial value that companies treat as confidential.

Trade secrets could potentially interfere with the deployment and use of DECODE technology.

f) Other intellectual property rights

The above list of the so called ‘intellectual property rights’ is not complete.

Other intellectual property rights exist (as way of example, geographical indications, plant varieties, etc.) but they do not seem to be relevant for DECODE technology.

1.2.2 Free licenses

Free software licenses emerged in the '80s as a legal tool to foster free software development and sharing.

More recently, other free licenses have been designed to foster the building of digital commons made up of creative works that are not software.

From a legal perspective, it’s useful to start from the beginning: the free software communities, i.e. the first communities that shaped practices and tools (including legal tools) fostering the creation of digital commons.

““Free software” means software that respects users’ freedom and community. Roughly, it means that the users have the freedom to run, copy, distribute, study, change and

³² Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure; see <http://data.europa.eu/eli/dir/2016/943/oj>

improve the software. Thus, “free software” is a matter of liberty, not price³³. The fact the free software is eventually distributed for a price does not change its nature.

According to the free software definition, “A program is free software if the program's users have the four essential freedoms:

- to run the program as you wish, for any purpose (freedom 0)
- to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this
- to redistribute copies so you can help your neighbor (freedom 2)
- to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

A program is free software if it gives users adequately all of these freedoms³⁴.

The availability of the source code (that is, the version of the software that can be analyzed and modified by developers) is central to the notion of free software. To run on computers, the software has to be translated into machine language capable of running on computers. This is made by an interpreter program or by a program that compiles the ‘object code’ (the software version that can be interpreted by computers but it is not understandable by developers).

Free software licenses are the legal tools that have been used since the 1980s to promote free software development and distribution: they are legal acts by which the author licenses copyrights and patent rights to allow users to enjoy the freedoms provided by the free software definition.

Therefore, for a program to be free software, it is enough that the right holder distributes it under the terms of a suitable license: a free software license that gives users the freedom to share, study and modify the software.

Generalizing the definition of free software, in this deliverable we will define free licenses the copyright (and, if applicable, patent) licenses that give users the freedom to share, study and modify the work they apply to.

1.2.2.1 Free licenses history

The notion of free software license, like the notion of free software, stems from some events that occurred between the 1970s and 1980s.

³³ See <https://www.gnu.org/philosophy/free-sw.en.html>.

³⁴ See <https://www.gnu.org/philosophy/free-sw.en.html>.

Today, it is natural to think of software as an artifact protected by copyright (and, in some countries, patent for invention).

But software (and therefore the debate about its legal protection) goes back in time just few decades.

In the 1960s software moved the first steps out of the research labs.

Until the '70s it was considered an accessory of computers (then made up of expensive mainframes) and circulated freely in universities according to the habit of free sharing of knowledge that characterize the prevailing scientific and academic ethos (at least at that time).

In those years, the idea that software could have an autonomous economic value separated from the hardware on which it is installed emerged, and in the United States (the country where IT was more developed) the issue about possible legal protection of software was debated.

In theory, there were two legal models that could protect software: copyright and patent right. After a long debate, the most flexible and least bureaucratic model of copyright was preferred.

From a practical perspective, the US Copyright Office had been accepting applications for software registration since 1964, but for several years still, the rules and jurisprudence did not offer any reliable grounds for arguing the extension of copyright to software. This situation of uncertainty ended in 1976 with a copyright reform that opened up to software protection and the debate finally ended in 1980 when the Computer Software Copyright Act was adopted.

Meanwhile, US courts ruled on the applicability of patent law for software invention: in 1981, the US Supreme Court, in the case *Diamond v. Diehr*, decided for the first time admitting software patentability.

In these years, personal computers and low-cost computing started to spread: the collapse of the hardware costs paved the way for the commercial software market.

In the meantime, in the USA, other events had a profound effect on the way in which US universities used to work in computer labs.

In 1980 a regulatory act was issued, the Bayh Doyle Act, which allowed universities to perform research activities jointly with commercial companies and to privatize research results.

Meanwhile, AT&T (a US telecommunications company), in order to achieve its goals as a telecommunications service management, fostered the realization of the UNIX operating system.

But AT&T was not allowed to market it: being a monopolistic company, AT&T was subject to some obligations imposed by the US antitrust authority, including the prohibition to sell UNIX.

Therefore, UNIX was freely available for US IT universities labs.

In 1980 AT&T was divided in different companies. As a consequence the ban on doing business in other sectors than telecommunications was over.

Since 1982, following the break-up of AT&T, UNIX was distributed under a commercial license.

In the early 1980s, as the proprietary software model was taking shape, the practice of software sharing, which was part of the practices of computer labs of US universities, was under attack.

In this context, the new paradigm of proprietary software was rejected by a relevant part of the developer community. In 1983, Richard M. Stallman founded the GNU Project with the aim to create a totally free operating system alternative to the UNIX system, no longer available for users (GNU is a recursive acronym that stands for "*GNU's not UNIX*"). Many developers joined Stallman's efforts and, thanks to the potential of the Internet network, the GNU Project grew quickly.

However copyright and patents severely limited the possibility to go on sharing, studying and modifying software.

The problem was tackled through new legal instruments: the free software licenses.

A program is released as free software if the right holder publishes it by applying a suitable license: a free software license.

In 1989, Richard Stallman wrote the first version of the GNU-GPL license (unifying similar licenses he used for earlier versions of his programs) that was followed by a second version in 1991 and a third version in 2007.

The GNU-GPL license was used for the programs of the GNU project.

Nowadays the GNU-GPL license is adopted by a large number of projects and it is at the heart of the free software movement.

Wide adoption of this license is partly due to historical reasons (it's the license created by Richard Stallman, the founder of the Free Software Movement) but also practical reasons: the engineering of this license favoured the spreading of free software.

In a nutshell, the GNU-GPL allows the user to modify and redistribute software licensed under this license provided that the modified version is in turn licensed under the terms

of the same license. It is the "copyleft" effect³⁵ that proved to be very attractive and favored the spreading of free software³⁶.

To cut to the chase, copyleft licenses foster sharing: whoever wants to modify the software and distribute it (or, sometimes, allow its remote use) can do so provided that he in turn gives the users the same freedoms that were granted to him. This is a hacking³⁷ of law that triggers virtuous spreading of free software by protecting users' freedom.

When in 1992 Linus Torvalds, a young Finnish student, made the Linux kernel available as free software (the operating system element that manages interactions between different parts of the computer: keyboard, screen, cpu, RAM, etc.), the new GNU-Linux operating system was complete.

The realization of the Linux kernel was a very important event in the spread of free software. Perhaps this is the reason why today, when we read the term Linux, we have to ask ourselves if it is used to refer to the kernel of the operating system or, according to a common synecdoche, to the entire GNU-Linux operating system (of which the kernel is just a part).

After the making of the Linux kernel, the potential of free software spread within the IT industry. The foundation by a group of developers of the Open Source Initiative, in 1998, played a major role³⁸.

The main goal of the founders for creating the new entity was avoiding emphasis on ethical aspects and use of the word "free" (that in English also means "without payment") which, in their view, hampered the understanding and use of free software by IT companies.

They used the term "open source" and adopted the Open Source Definition, that, substantially, reproduces the free software definition with a different formulation³⁹.

The term open source focuses on the requirement of access to the source code of the software: the Open Source Initiative does not mention ethical aspects and focuses on the development model of free / open source software.

The Free Software Foundation (founded by Richard Stallman) releases a list of licenses that comply with the definition of free software⁴⁰.

³⁵ Copyleft as opposite to copyright.

³⁶ The copyleft effect is not essential to the notion of free software. Actually, there are free software licenses that are not copyleft licenses.

³⁷ Hacking means finding (and enjoying finding) creative solutions to problems. This term is popular among developers.

³⁸ See <https://opensource.org/>.

³⁹ See <https://opensource.org/osd>.

⁴⁰ See <https://www.fsf.org/>, <https://www.gnu.org/licenses/license-list.html>, <https://www.fsf.org/about/what-is-free-software>.

Like the Free Software Foundation, the Open Source Initiative publishes a list of licenses⁴¹ that comply with the Open Source Definition.

Even if the two definitions are worded in a different way, they point to the same goal: identify licenses that foster sharing, studying and modifying the software.

It's a matter of fact that the two lists of licenses are considered to be substantially coincidental, except for a few differences for specific licenses, all depending on minor details and not to substantial issues⁴².

Nowadays there are many free software licenses (although the most commonly used are relatively few: the 10 most common licenses are adopted by more than 90% of the free software projects)⁴³.

The free software model has inspired attempts to reproduce its dynamics in other areas of human activity and has led to the creation of new licenses for digital commons made of non-software works (newspapers, books, music, videos, databases, electronic designs, etc.).

Among these attempts, the case of the Creative Commons Public Licenses certainly deserves to be mentioned: although it was not the first attempt to create standard licenses for works other than software, it was certainly the most successful.

They were written by the Creative Commons Corporation, a US non-profit organization. Creative Commons Public Licenses are 6 modular copyright licenses, consisting of the combination of four options:

- Attribution (BY): credit must be recognized to the author of the work,
- Share-alike (SA): any work that modifies the work licensed must be distributed under the terms of the license that applies to the work licensed,
- Non-commercial (NC): the work can not be used for profit or business purposes,
- No Derivative Works (ND): distribution of works that modify or transform the original work is not allowed.

The Attribution option is mandatory since version 2.0 of the Creative Commons Public Licenses (the latest version is 4.0).

No Derivative and Share-alike options are logically incompatible and cannot coexist as they affect (in a different way) the same faculty of distributing works that modify the original work.

Thus, the combination of the 4 options drives to 6 licenses:

- Attribution,
- Attribution – No Derivative works,

⁴¹ See <https://opensource.org/licenses>.

⁴² See https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses#Approvals.

⁴³ See <http://www.blackducksoftware.com/oss/licenses#top20>.

- Attribution – Share-alike,
- Attribution – Non-commercial,
- Attribution – Non-commercial – No Derivative works,
- Attribution – Non-Commercial – Share-alike.

Creative Commons Public Licenses are designed to give the author the freedom to choose the license that best suits his purposes.

But, on the one hand, the Non-Commercial option prevents users from using the work for commercial purposes and, on the other hand, the Non-derivative option does not allow the user to modify the work, thus diverging from the list of freedoms ordinarily conferred by free software.

This difference has been highlighted by the promoters of the definition of Free Cultural Works⁴⁴, according to which only two of the Creative Commons Public Licenses are free cultural works licenses: the CC Attribution license and the CC Attribution-Share-alike license.

Creative Commons Corporation has also made available CC0, a declaration of renunciation to copyright on the work⁴⁵.

As a matter of fact, CC Attribution and CC Attribution-Share-alike licenses and CC0 public domain dedication have been helpful in generating digital commons. For example, the Creative Commons Attribution Share Alike license is currently used for Wikipedia⁴⁶.

In recent years, an increasing number of projects have aimed to foster the creation of digital commons that consist of databases, including different governments that started releasing public databases under the terms of free licenses.

CC Attribution, CC Attribution-Share-alike, and CC0 licenses have been used for databases, but new free licenses, specifically designed for databases, were also created, such as the licenses made by the Open Data Commons⁴⁷, including the Open Data Commons Open Database License (Odbi)⁴⁸, that is used for the OpenStreetMap project⁴⁹.

More recently, efforts to create digital commons related to the production of material objects (electronic cards and other material objects) have intensified.

It is useful to divide the domain of design material objects into two subcategories: on the one hand,

⁴⁴ See <http://freedomdefined.org/Definition>.

⁴⁵ See <https://creativecommons.org/publicdomain/zero/1.0/legalcode>.

⁴⁶ See <https://www.wikipedia.org/>.

⁴⁷ See <https://opendatacommons.org/>.

⁴⁸ See <https://opendatacommons.org/licenses/odbi/>.

⁴⁹ See <http://www.openstreetmap.org/copyright>.

electronic circuit boards, on the other hand the other material objects.

The distinction is useful for historical reasons: the digital commons movement related to electronic circuit boards is much older (also due to the greater cultural proximity to the free software communities).

The interest on the realization of digital commons related to the production of different kind of material objects has developed in recent years, after the spread of low cost 3D printers.

The distinction is also useful for practical reasons: normative frameworks insisting on the two classes of artifacts are different. On one hand, electronic circuit boards may be the subject of the right on layout design of integrated circuits; on the other and, rights related to the form of the object (such as the industrial design right or copyright) may insist on other material objects.

Communities that work for the creation of digital commons related to the manufacturing of material objects must then handle other problems rather than those solved by communities that develop free software.

First, they must verify that the free license they choose to use properly manages the regulatory frameworks involved with the type of artifact they intend to make.

This issue pops up for electronic circuit boards: the GNU-GPL licenses rights on layout design of integrated circuits, but not all the free licenses are designed to achieve this result.

Communities licensing electronic circuit board designs also faced the problem of ensuring that anyone who buys an electronic circuit boards can have access to the design of the same board. To achieve this result (not achievable with free software licenses), two new free licenses were created, specially designed for electronic circuit boards: the *CERN Open Hardware Licence*⁵⁰ and the *TAPR Open Hardware License*⁵¹.

Rights of industrial design (possibly insisting on designs of other material objects) may require the creation of new licenses or adaption of existing licenses⁵².

But an effective strategy of building digital commons related to the design of material objects may require to take into account other aspects.

The transition from the digital design of a material object to its manufacturing requires to take into account other regulatory frameworks, such as those requiring compliance with specific safety standards or to obtain certifications. Taking into account the

⁵⁰ See <http://www.ohwr.org/projects/cernohl/wiki>.

⁵¹ See <http://www.tapr.org/ohl.html>.

⁵² Margoni, T. "Not for Designers: On the Inadequacies of EU Design Law and How to Fix It" *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 4-3 (2013). 225-248. Accessed May 16, 2017. <http://www.jipitec.eu/issues/jipitec-4-3-2013/3845/margoni.pdf>.

regulatory frameworks that interfere with the manufacturing of material objects since the design phase, can allow to reduce manufacturing costs.

For example, in the EU funded UBORA project⁵³ for the design of biomedical devices, it was found useful to couple the open design strategies with the adoption of procedures for respecting quality assurance, and assessing performance and safety as required by applicable laws.

Artificial Intelligence is another area where utility “*per se*” of adopting free software licenses is questioned.

There are different projects releasing free software that implement a variety of machine learning algorithms and/or preset models for using software implemented machine learning algorithms. For example, the TensorFlow project⁵⁴ (a free software library for numerical computation using data flow graphs) adopts the Apache License v. 2 for its software and models⁵⁵.

Whether licensing software and models under free software licenses is the most efficient strategy to foster generation of digital commons in the domain of machine learning, however, is still an open question.

Some issues have to be considered.

At least in some countries outside EU (including USA), applicability of copyright to models (sometimes consisting in plane dataset structures) is questioned: this poses the problem of the enforceability of free software licenses on such models.

Moreover, looking from a wider angle, often machine learning is performed through the processing of personal data and/or of data that, even if are not personal data, are provided by natural persons.

From the perspective of the data subject or data provider (whose data is used, with other data, to perform machine learning and who uses the machine learning algorithm), having access to a digital common could entail more than just having access to the source code of the software and to the model adopted for the machine learning algorithm.

For example, the data subject could be interested in understanding the characteristics of the data that are used by the machine learning algorithm in order to be able to evaluate if the algorithm is effective and/or biased.

⁵³ See <https://uboratest.wordpress.com/>.

⁵⁴ See <https://www.tensorflow.org/>.

⁵⁵ See <https://github.com/tensorflow/models> adopting Apache license.

1.2.2.2 Free licenses characteristics

As already pointed out, the most relevant aspect of free software licenses is whether or not they include a copyleft clause.

The “copyleft” clause is not the same in different free software licenses: it produces different effects depending on its wording.

This is why free software licenses are classified according to how the copyleft feature works in each license.

First, there are non-copyleft licenses, i.e. licenses (such as the BSD⁵⁶, MIT⁵⁷ and Apache⁵⁸ licenses) that do not contain a “copyleft” clause and therefore have no “copyleft” effect: who distributes a software available under a “non-copyleft” license is not required to distribute it under the terms of the same license.

Then, there are the so-called “strong copyleft” licenses: these are licenses that contain copyleft clauses extending their effects to all derivative works, including software libraries that, when executing a software licensed under a “strong copyleft” license, are linked dynamically to it⁵⁹.

The licenses that, however, narrowly restrict the scope of the “copyleft” clause, thus allowing different licenses to be applied to some derivative works, are called “weak copyleft” licenses; among them the GNU Lesser General Public License (GNU-LGPL)⁶⁰ and the Mozilla Public License (MPL)⁶¹.

There are also some licenses, such as the GNU General Public License (GNU-AGPL)⁶² and the European Union Public License (EURL)⁶³, which requires that the source code of the program is available also to users who use the software remotely, connecting to the server at which the software is run as a service (called SaaS): these licenses are called “network copyleft”.

In some countries, software may also be subject to patent right for invention that awards to the holder the exclusive right to implement the invention and to profit from it.

⁵⁶ There are different versions, the last of them is the one adopted for the project FreeBSD (see <https://www.freebsd.org/copyright/freebsd-license.html>).

⁵⁷ See <https://mit-license.org/>.

⁵⁸ For the last version 2.0 see <https://www.apache.org/licenses/LICENSE-2.0>.

⁵⁹ On the extension of the copyleft effect of the strong copyleft licenses there are different opinions (see <http://www.ifosslr.org/public/LinkingDocument.odt> cited in Bain, 2010).

⁶⁰ For the last version 3.0 see <https://www.gnu.org/licenses/lgpl-3.0.en.html>.

⁶¹ For the last version 2.0 see <https://www.mozilla.org/en-US/MPL/>.

⁶² For the last version 3.0 see <https://www.gnu.org/licenses/agpl-3.0.html>.

⁶³ For the last version 1.2 see https://joinup.ec.europa.eu/community/eupl/og_page/eupl-text-11-12.

Whoever uses or distributes free software can not exclude that that software interferes with a patent-protected invention.

The use and diffusion of free software is thus also affected by patent law.

In some free software licenses, various techniques are used to limit patent interference with free software and to discourage who wants to prevent the use and distribution of free software by claiming a patent.

For example, some licenses provide that whoever contributes to the software and/or who distributes it (as the case may be) licenses its (if any) patent rights.

1.2.2.3 Free software licenses: some considerations for the DECODE project

The free software socio-technological system is certainly the most mature environment in terms of generation of digital commons: many free software projects are digital commons⁶⁴.

It is therefore useful to make some considerations about the path that drives free software to become digital commons looking for hints about how achieving the result of fostering the creation of digital commons within DECODE, even if DECODE is more than just software.

As a whole, the free software socio-technological system consists of a large number of programs⁶⁵ and the range of relationships that are built with these programs between a large number of people (developers and users), companies, public and no-profit organizations.

Applying a free software license to a program does not make “*per se*” that program a digital common; a program that is free software is a digital commons if further conditions are met (including existence of a relevant community of developers and users of the program). Nonetheless, the fact that the program is licensed under a well known free software license seems to be the first step towards the creation of a digital commons: free software licenses are more easily accepted by developers and users.

People who develop and use free software can do it on their own or in the interest of companies or organizations they work for.

Choosing to develop or to use free software for ethical reasons is unusual for companies. It is more typical with people who act on their own and (assuming that their goals can qualify as ethical goals) with public and no-profit organizations.

⁶⁴ For a discussion on the definition of digital commons see *Annex A* of this document.

⁶⁵ On the website <https://www.openhub.net/explore/projects> more then 650.000 projects are listed.

It is a fact that in the early '80s the creation of free software was based on ethical reasons as a reaction to the emergence of the new paradigm of proprietary software. Richard Stallman says: “*My work on free software is motivated by an idealistic goal: spreading freedom and cooperation. I want to encourage free software to spread, replacing proprietary software that forbids cooperation, and thus make our society better*”⁶⁶.

Starting from that original ethical drive, free software socio-technological systems have evolved and today subjects with very different goals from those who gave birth to the original design of free software are participating in these systems.

Nevertheless, free software licenses played a key role in the growth of digital commons made of software.

Free software development projects (sometimes institutionalized within legal entities, sometimes not) have been organized around free software licenses, and such free software development projects interact among themselves and exchange data, functions and code, sometimes in an organized way, sometimes not.

The free software socio-technological system, as a whole, is not centrally coordinated.

It is therefore possible to suppose that free software licenses work as means of communication apt to foster stigmergic behaviour, that is indirect coordination: the free software licenses have been the generative/genetic code of the socio-technological system that self-organized around them, creating software digital commons (Elliot, 2006).

Single software projects that become digital commons, on the other hand, use to be minimally organized (even when they are not institutionalized in entities), at least through the use of the technologies adopted to develop them.

From the point of view of a single free software project, free software licenses are effective tools that allow solving problems typically handled by legal acts (laws, contracts, etc.). They allow to (a) eliminate uncertainty, (b) minimize transaction costs and (c) reallocate risk:

- a) eliminate uncertainty: free software licenses are well known and recognized in the communities of free software developers and users (the fact that a program is available under the terms of a certain free software license makes it easy for the users to identify their rights and obligations);
- b) minimize transaction costs: use of a free software license, instead of a license drafted *ad hoc*, reduces the costs associated with the adoption of the license;
- c) reallocate risk: if a program is available under the terms of a free software license, the user can reasonably assume that the distributor did not deliberately include code in violation of third party rights.

⁶⁶ See <https://www.fsf.org/licensing/essays/pragmatic.html>.

In short, **free software licenses are efficient in building trust** among the people involved in the socio-technological systems that are built around free software projects and from the legal efficiency of the free software licenses follow social, economic, and other relevant effects.

Some further considerations from a legal perspective could be useful.

Copyleft clauses are usually adopted by communities of developers particularly motivated by ethical goals of protecting users' freedom and encouraging sharing⁶⁷.

But such ethical goals are not shared by all developers in all circumstances.

The interest of some stakeholders to avoid the copyleft effect led to creation and adoption of different non-copyleft and weak copyleft licenses.

Moreover, free software licenses do not solve all the legal problems. In some cases, some of these problems involved different solutions and adaptations with aim to guarantee the growth of the socio-technological system of free software.

For example, free software licenses are objectively inappropriate to radically solve the problem posed by patent rights⁶⁸.

For this reason, a few years ago a patent pool involving the major players in the industry that awards all Linux kernel users a license on the patents held by all the members of the pool was established⁶⁹.

There are other legal frameworks that may be involved with the use and distribution of free software (such as trademark rights, right to technological protection measures, or right on secret information). In some cases, a solution for the management of these legal frameworks was found within the free software licenses or with the adoption of new legal acts.

In other cases, communities of developers and users adopted and refined community practices and technologies that maximize freedom and collaboration (software versions management systems, bug reporting systems, open formats, license compliance and enforcement practices, etc.).

For example:

- the Software Package Data Exchange (SPDX) format was developed to

⁶⁷ Incidentally, it's interesting to notice that both the Creative Commons Attribution Share Alike license (adopted for Wikipedia) and the Open Data Commons Open Database License (adopted for OpenStreetMap) are copyleft licenses: this could suggest that preference for copyleft licenses moved from communities working on software digital commons to communities working with non-software digital commons.

⁶⁸ Usually, free software licenses provide for express or implied license of patent rights. Some licenses provide for additional legal techniques of some effectiveness. For example, the MIT license provides for a retaliation clause in case the user claims patents; or, the GPLv3 license provides for clauses to prevent patent-related agreements.

⁶⁹ It refers to the Open Invention Network (see <https://www.openinventionnetwork.com/>).

standardize (and thus automatically identify) the licensing information that applies to free software⁷⁰;

- recently, the Linux Foundation promoted the OpenChain initiative, with the aim of offering a benchmark to support who distributes free software to perform compliance with free software licensing provisions and thus improve the overall conduct of the various actors⁷¹;
- to handle the issue of trademark law, specific trademark policies have been created complementing free software licenses for specific projects.

In conclusion, free software licenses worked, with other tools, to meet the ethical needs of the communities involved with the development and use of free software: as a result, to be successful, the DECODE Project should implement tools that meet the ethical needs of the communities involved by the development and use of the DECODE technology.

1.2.3 Distributed ledgers architectures and intellectual property rights

The deployment of the DECODE technology through distributed ledgers poses additional questions concerning intellectual property rights.

Particularly, one could question whether the datasets formed within a distributed ledger technology are protected by copyright and *sui generis* right on databases.

Moreover, it cannot be excluded that the database stored in the distributed ledger consists of works protected by copyright.

Last but not least, the software to be used by the peers of the network to run the distributed ledger peer could be the subject of copyright and (for the countries where software patent apply) of patent right.

Adoption of free licenses for the software to be implemented and for databases to be used within the DLT of the DECODE technology is fundamental to maximize the chance that digital commons will emerge out of the DECODE project.

These issues will be considered in the next sections in order to identify possible measures and strategies.

⁷⁰ See <https://spdx.org/>.

⁷¹ See <https://www.openchainproject.org/>.

1.3 Privacy and data protection law

DECODE shall be designed to be compliant with the data protection and privacy legal framework. Here we focus on the design of the DECODE technology (specific use of DECODE technology, within pilots or other uses, are not addressed in this document).

1.3.1 EU legal framework & highlights

The European Union legal framework on privacy and data protection has been largely made up by Directive 95/46/EC for the past two decades. In 2016, Regulation 2016/679 (General Data Protection Regulation) was passed. Regulation 2016/679 replaces Directive 95/46/EC, and “lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data” (Article 1(1)). It will enter into force on 25 May 2018 after a two-year transition period and, unlike a directive, it does not require any enabling legislation to be passed by Member States and is thus directly binding and applicable. Until May 2018, Member States should change and adapt their own legislations in order to make them compatible with the new Regulation.

Nonetheless it is necessary to remind that rules on privacy and data protection rights, as enshrined in ECHR, Article 8, are not limited to the GDPR, but also include other rules (e.g. the e-Privacy Directive⁷², Directive (EU) 2016/680) and national rules that could overlap with privacy and data protection rights.

In this document we will consider the rules that are provided by the new GDPR, since it sets up definitions, principles and obligations that will specify the general data protection framework.

1.3.1.1 The notion of personal data

Article 4 provides for the definitions of Regulation 2016/679. It establishes some key definitions, such as: personal data, data subject, data processing, consent of the data subject, pseudonymization, data controller and data processor.

According to Article 4(1), point 1:

⁷² Directive 2002/58/EC. This Directive is currently under review, see the Proposal for a new E-Privacy Regulation (2017, EC).

“‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’)”, who is the identified or identifiable natural person which the data is referring to.

The same Article adds that:

“An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”⁷³.

‘Direct identification’ means identification of the respondent from their formal identifiers (name, address, identification number) and ‘indirect identification’ means inferring a respondent’s identity by a combination of variables or characteristics (e.g. age, gender, education etc)⁷⁴.

The principles of data protection should apply to any information concerning an identified or identifiable natural person. *Vice versa*, the principles of data protection and the rules provided by the GDPR should not apply to ‘anonymous’ information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable⁷⁵.

Recital 26 adds that *“To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments”*.

⁷³ This means, for example, that also email address and IP address shall be regarded as personal data.

⁷⁴ See also Recital 30 that adds more information about identifiers: *“Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them”*.

⁷⁵ On the concept of anonymisation, see the Working Party Article 29, *Opinion 05/2014 on Anonymisation Techniques* (wp 216).

1.3.1.2 General principles and definitions on personal data processing

Concerning the applicability of the rules provided by GDPR, it is crucial to stress the meaning of 'personal data processing'. According to Article 4(1), point 2, personal data processing means:

"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

Any personal data processing should be lawful and fair, according to the principles set out by Article 5, such as lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality⁷⁶.

Personal data *"shall be processed lawfully, fairly and in a transparent manner in relation to the data subject"*. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. This principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.

Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. Moreover, personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

The principle of data minimisation means that *"personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed"*. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. In order to ensure that the personal data are not kept longer than necessary, data should be kept in a form which permits

⁷⁶ See also GDPR, Rec. 39.

identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Time limits should be established by the controller for erasure or for a periodic review.

Personal data shall be *“accurate and, where necessary, kept up to date”* (accuracy principle), and *“every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted”*.

Finally, personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful processing (such as unauthorised access to or use of personal data) and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In order for processing to be lawful, unless other specific conditions or exceptions apply⁷⁷, personal data should be processed on the basis of the consent of the data subject concerned (Article 6(1)): *“the data subject has given consent to the processing of his or her personal data for one or more specific purposes”*. The definition of ‘consent of the data subject’ is provided by Article 4(1), point 11, and it *“means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”*. Recital 42 adds that *“For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment”*.

Furthermore, it is important to remind that a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using

⁷⁷ Article 6(1) of the GDPR lists the following conditions:

“Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.

Paragraphs 1-4 of the same Article provide exceptions to the mentioned conditions.

clear and plain language and it should not contain unfair terms (see Directive 93/13/EEC).

The consent to the data processing can be withdrawn at any time. This is a right of the data subject, according to Article 7(3). Anyway, the “*withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal*”. Moreover, “*it shall be as easy to withdraw as to give consent*”.

1.3.1.3 Data subject's rights

The data subject has the right to be informed in a complete and plain way about the processing of data relating to him or her, according to the principles of transparency.

Accordingly, the data controller (the entity that determines the purposes, conditions and means of the processing of personal data⁷⁸, *infra*) has the duty to provide such information, as stated in Articles 12, 13 and 14 of GDPR. The controller shall provide the data subject with any information on the existence and the purpose of the data processing, and any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context of the data processing.

Pursuant to Article 12(1), the information should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Such information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

Article 13 defines the content of the information the data controller should provide the data subject for the case in which personal data are collected directly from the data subject. Article 14 defines the content when personal data have not been obtained from the data subject.

The information should be given to the data subject at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case (see Article 14(3)). Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Moreover, where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other

⁷⁸ Article 4(1), points 7 and 8 of the GDPR provides for the definition of data controller as follows: data ‘controller’ is the “*natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*”.

necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided⁷⁹.

Within DECODE, the information could be provided through 'smart rules' at the time the participant will join the service based on the DECODE technology or whenever it is necessary according to Articles 13 and 14 of GDPR.

The information provided by the controller according to Articles 12, 13 and 14 will facilitate the data subject to exercise his or her rights under Articles 15 to 22.

The data subject's rights are:

- Right of access by the data subject (Article 15(1)):

"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data" and information about the processing⁸⁰;

- Right to rectification (Article 16(1)):

"The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement";

- Right to erasure ('right to be forgotten') (Article 17):

"(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the

⁷⁹ See GDPR, Rec. 61.

⁸⁰ Article 15(1) lists the information the data subject's has the right to obtain, such as:

"1. the purposes of the processing;

2. the categories of personal data concerned;

3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

5. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

6. the right to lodge a complaint with a supervisory authority;

7. where the personal data are not collected from the data subject, any available information as to their source;

8. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".

controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject withdraws consent on which the processing is based (...) and where there is no other legal ground for the processing;
- c) the data subject objects to the processing pursuant to Article 21 (...);
- d) the personal data have been unlawfully processed;
- e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data⁸¹.

- Right to restriction of processing (Article 18):

“(1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

⁸¹ Paragraph 3 of Article 17 adds exceptions to the application of paragraphs 1 and 2: “Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- e) for the establishment, exercise or defence of legal claims”.

d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

(3) A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted".

- the Right of Notification by the controller about rectification or erasure of personal data or restriction of processing (Article 19)⁸²
- Right to data portability (Article 20(1)):

"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- 1. the processing is based on consent (...); and*
- 2. the processing is carried out by automated means"*⁸³.

- Right to object (Article 21(1)):

"The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the

⁸² Article 19 provides: "The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it".

⁸³ Recital 68 clarifies that "By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible".

processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims”.

- Automated individual decision-making, including profiling (Article 22):

“(1)The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) Paragraph 1 shall not apply if the decision:

- 1. is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
- 2. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or*
- 3. is based on the data subject’s explicit consent.*

(3) In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision”.

These provisions are extremely important for the data controller, who has the obligation to take action on request of the data subject for the exercise of those rights, also providing the information requested (according to Article 12(2-3)).

Nonetheless, it is worth mentioning the exception to these obligations of the data controller, in the cases in which data processing does not require identification of the data subject, pursuant to Article 11:

“(1) If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

(2) Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification”.

This provision could have a strong impact on the obligations of the data controller whenever the latter can demonstrate his impossibility to identify the data subject.

The applicability of this Article and the exemptions it provides are closely related with the concepts of anonymisation and pseudonymisation.

1.3.1.4 The control of the data processing, obligations and responsibilities

Article 4(1), points 7 and 8 of the GDPR provides for the definition of data controller and data processor:

- data 'controller' is the "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"; while the
- data 'processor' is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"⁸⁴.

As to the data controller, Article 24(1) determines: "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation (...)".

As to the duties and responsibilities of the data processor vis a vis the data controller, Article 28(3) sets up the following: "Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller". This Article also lists the content of the legal act which defines those responsibilities⁸⁵.

⁸⁴ See also Opinion 1/2010 on the concepts of "controller" and "processor", adopted by the Working Party Art. 29 (wp169).

⁸⁵ "That contract or other legal act shall stipulate, in particular, that the processor:

- (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) takes all measures required pursuant to Article 32;
- (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
- (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
- (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

Article 26 provides that “where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers”. In this case they should determine their respective duties and responsibilities in accordance with the GDPR. In the context of DECODE this arrangement could be embedded into smart rules. Their respective roles and relationships shall be defined by an arrangement, that shall be made available to the data subject.

The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, according to Article 24, the controller has to implement appropriate and effective measures and shall demonstrate the compliance with the GDPR of processing activities, including the effectiveness of the measures.

Thus, the main obligations of the data controller are to:

- process data lawfully, that is with the consent of the data subject, unless other conditions or specific exceptions apply (Article 6);
- provide the data subject of the information related to the data processing (Articles 12-14);
- keep the necessary actions in order to safeguard the exercise of the data subject’s rights under Articles 15 to 22;
- adopt privacy by design and privacy by default measures (Article 25);
- keep record of processing operations (Article 30);
- adopt security measures (Article 32);
- provide notification of a personal data breach to the supervisory authority and communication of the data breach to the data subject (Articles 33 and 34);
- provide a Privacy Impact Assessment (PIA) where it is necessary (Article 35)
- designate a Data protection Officer (DPO) where it is necessary (Article 37).

The obligation to single out the appropriate means and measures for the personal data processing in order to ensure its security and the safeguards of the rights and provisions required by the GDPR, is crucial within the context of DECODE.

To ensure that those requirements are met the data controller shall adopt privacy by design and privacy by default measures⁸⁶.

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions”.

⁸⁶ Since the late '90 the principle of privacy by design was introduced by Ann Cavoukian (Cavoukian, 2010) and its popularity in the European legal framework started with the document “The Future of Privacy” (02356/09/EN – wp168) adopted on December 1st, 2009 by EU Article 29 Data Protection Working Party (WP29) and the Working Party on Police and Justice (WPPJ). In 2012 it was included in the Proposal of revision of the Directive 95/46/EC, and, finally, it was

Article 25(1) of GDPR provides that the controller shall implement appropriate technical and organisational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

This obligation should be fulfilled *“taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing”*.

The data controller shall adopt privacy by design technical and organizational measures *“both at the time of the determination of the means for processing and at the time of the processing itself”* (Article 25(1) of the GDPR). This distinction aims to underline the necessity of pursuing privacy preserving goals both in the design phase and during the entire processing. It follows that there are 2 different obligations of the data controller:

- a) the responsibility for the determination of the technical and organizational measures to ensure the compliance of the data processing with data protection rules (see also Articles 7, 24, and 32);
- b) the responsibility for the implementation of those measures during the entire processing.

As to the responsibility in determining the means for the data processing, it is important to stress that when the data controller specifies the technical means, i.e. a technology, a platform, a software product and so on, he is still responsible for the consequences of the adopted means on both the processing and the data subject’s rights.

Generally, producers and developers of technical means for processing data are not responsible for their use. However, the GDPR recommends and encourages them to design the technology in such a way that they fulfil the requirements for ensuring data protection rights as provided by the new Regulation. Recital 78 states that *“When developing, designing, selecting and using applications, services and products that are*

enshrined in Article 25 of the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, that introduces legal obligation to design strategies. For a full comprehension of the implications of the PbD principle, it should be interpreted in accordance with the recommendations by Working Party Article 29 and by the European Data Protection Supervisor (see EDPS opinion on privacy in the digital age: “Privacy by Design” as a key tool to ensure citizens' trust in ICTs), and taking advantages from the standards and principles stressed by the International Standard Organization (ISO 29100).

A detailed review of tools and strategies of privacy by design for the DECODE Project is provided by D1.2 “Privacy Design Strategies for the DECODE Architecture”: S. Bano, E. Bassi, M. Ciurcina, A. Freire, S. Hajian, J.-H. Hoepman (2017). Privacy by Design Strategies for DECODE Architecture, and *infra* in the following sections.

based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations”.

The technical and organizational measures that the data controller shall adopt could consist of pseudonymising data or minimising the processing of personal data. He shall ensure *“that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons”* (Article 25(2)).

Pseudonymisation refers to the processing of personal data *“in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”* (Article 4(1), point 5). Moreover, Recital 26 of the GDPR stresses and clarifies the nature of pseudonymous data, stating that *“Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person”*.

Article 25 mentions pseudonymisation and data minimisation as examples of privacy by design measures, but the list is longer and includes security measures, encryption, anonymisation, noise aggregation, third parties limitation access, tools for ensuring data subject's informed consent and data subject's rights.

These measures are not alternative but could be adopted jointly⁸⁷. There could be strategies, patterns and tools that can work simultaneously to attain specific goals in preserving and in enforcing privacy rights.

⁸⁷ Some measures could be described as self-enforceable, while others are directed to conduct or to change user's behavior; see U. Pagallo (2012b). On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In Gutwirth S., Leenes R., De Hert P., (eds.) *European Data Protection: In Good Health?*, pp. 331 – 346. Moreover, some scholars distinguish between measures adopted by code and measures adopted by policy (or by communication (see for instance Pagallo, U. (2012b). On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In Gutwirth S., Leenes R., De Hert P., *European Data Protection: In Good Health?*, pp. 331 – 346 Koops B-J., Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law'. In: *International Review of Law, Computers & Technology* (28), 2, pp. 159-171).

Moreover, according to Article 32, the data controller has a specific obligation to adopt appropriate security measures. Recital 83 clearly explains that:

“In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage”.

1.3.2 Distributed Ledgers Architectures & privacy issues to be faced

Distributed Ledgers Architectures and Blockchain technology offer new opportunities for giving people the control of their personal data, allowing to choose what data they want to share and how⁸⁸. In addition, Distributed Ledgers Technologies can enforce the transparency of the data processing, as required by the GDPR’s Article 5(1), point a, Article 12 and Article 30 on records of processing activities. Also DLT can increase data integrity and confidentiality (Article 5(1), point f).

Still, Distributed Ledger Technologies (DLT) raise several legal questions that need to be answered. Most of them deal with privacy and data protection and can be summarized as follows⁸⁹. First, although personal data can be encrypted, DLT *“transactions involve personal data and are not fully anonymous”*⁹⁰. In many cases, albeit personal data *“is normally encrypted and can only be accessed with the correct keys, encryption of the data as such – i.e. giving access only to authorised parties – will normally not take such data out of the scope of the GDPR and may even be required. Even if personal information only entails reference ID numbers, such identifiers are*

For the idea of modularity of design see Hoepman, 2014 and Colesky et al., 2016; see also : S. Bano, E. Bassi, M. Ciurcina, A. Freire, S. Hajian, J.-H. Hoepman (2017). Privacy by Design Strategies for DECODE Architecture.

⁸⁸ This is the key objective for the DECODE Project, as well as for the ENIGMA Project by MIT; see G. Zyskind, O. Nathan, A. Pentland (2015). Decentralizing privacy: Using blockchain to protect personal data. Security and Privacy Workshops (SPW), 2015 IEEE.

⁸⁹ See G. Zyskind, O. Nathan, A. Pentland (2015). Decentralizing privacy: Using blockchain to protect personal data. cit.; Berberich M., Steiner M. (2016). Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?. *EDPL* (3), pp. 422-426.

⁹⁰ Berberich M., Steiner M. (2016). Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?. cit., 423.

*typically unique to a specific person. While in all such cases additional information may be necessary to attribute information to the data subject, such information would be merely pseudonymised and count as personal information*⁹¹. In addition, Berberich and Steiner claim that “A connection between pseudonymised data and the data subject will usually (and necessarily) arise in BC transactions effected for off-chain goods, e.g. conversion into real money payments, purchase of goods or services, registration data, where the transaction parties must be known. Against that background, there is a strong case for arguing that individual-related information on BC is personal data”⁹².

A second set of problems arise from the decentralization of DLT. Difficulties may concern either the individuation of a data controller, or ensuring the possibility of control by a supervisory authority (as prescribed by Articles 51ff. of the GDPR), so that fulfilling the obligations of the data controller can be really problematic in cases of data breach (according to Article 34 of the GDPR).

In managing these issues and allocating responsibilities for personal data processing, the key issue seems to be the individuation of the data controller or of multiple data controllers that could be jointly responsible⁹³.

Other issues hinge on the technical architecture of DLT and the persistence of all the stored transactions in such architecture. The principles of data minimisation and storage limitation, which are required for a lawful data processing, may be in conflict with the characteristics of DLT storage.

Berberich and Steiner stressed the point, suggesting the adoption of *ad hoc* Privacy by Design technology: “*in principle, BC embodies an inherent tension: At one hand, some of its features like perpetual distributed storage and the lack of central entities (in public BC models) could be seen as not completely in line with data minimisation and accountability. In respect of the latter, it could therefore make a difference whether public or private BC models are used. At the other hand, a strong BC encryption and data security would be in line with PbD. Against this background, an approach to mitigate this tension and to tip BC more towards the safe zones of data protection may lie in implementing additional PbD compatible technology. This may include eliminating ways that would allow tracking back pseudonyms to individual users, or adding ‘noise’ to BC data so that transactions are mixed up. Another promising idea is to combine on-*

⁹¹ Berberich M., Steiner M. (2016). Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?. *ibidem*.

⁹² Berberich M., Steiner M. (2016). Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?. *ibidem*.

⁹³ Berberich and Steiner distinguished “*between ‘private BC’ and ‘public BC’*” and for the case in which “*the use of BC is also tested in closed groups of ‘trusted’ entities (...) one can easily imagine regulators to focus on either a technical system operator (if any, eg a joint venture set-up) or consider the group of participating entities as joint controllers*”. Berberich M., Steiner M. (2016). Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?. *cit.*, 424.

*chain and off-chain storage for more sensible data and using BC only as a 'pointer' to centrally stored data, as it is the case in the MIT 'ENIGMA' project, which uses modified distributed hash tables for storing secret-shared data in combination with an external BC for network, access and identity control*⁹⁴. Last but not least, the persistence of all transactions may cause tensions with the right to rectification and the right to be forgotten provided by the GDPR and is waiting for new solutions.

In short and following a proactive approach, DLT and smart rules could offer a new scenario for designing and inventing new tools and strategies for allowing privacy and data protection safeguards. One first example is the possibility to use smart rules to personalize the conditions of personal data sharing, and to improve transparency in the definition of responsibilities⁹⁵.

1.4 Other limitations to data sharing and reuse

In this section we mention some other limitations to data sharing and reuse. Limitations on data sharing and reuse can be set up to protect specific rights of a third party or to pursue the public interest in assuring confidentiality and secrecy for specific domains and sectors according to national legislations. Those limitations entail what data can be shared within services and activities based on distributed ledger architectures as DECODE OS.

1.4.1 Rights of the personality and other rights

Certain other rights (in addition to IPRs and privacy rights) could regard immaterial goods and therefore to data.

The content of such rights is not harmonized through different countries and differences tend to widen among countries with different cultural background.

In general, such rights could be divided in two categories: rights that are protected by law (from which arise obligations for third parties) and rights that are protected by contract (from which arise obligations to the parties of each specific contract).

⁹⁴ For the ENIGMA project solutions, see G. Zyskind, O. Nathan, A. Pentland (2015). Decentralizing privacy: Using blockchain to protect personal data. cit.

⁹⁵ A detailed description of those tools that may be adopted will be provided in D1.9 "Licensing of digital commons including personal data".

There are different circumstances under which, even if intellectual property rights or privacy rights do not apply, one could not be allowed to use data because their use interferes with a right of a third party.

This includes the case where such data violate the so called rights of personality of a third party (as an example, right to image, right to identity, right to the name, right to honor). The list of this rights and its content depends on the national legislation that applies and strongly on the cultural perspective of the different countries.

For example, the circumstances under which one could legitimately diffuse information that damage the reputation of a third party (committing or not defamation) depend on how national legislation and judges may interpret the balance between the freedom of speech and the right to privacy and honour of the interested person.

Some other rights limiting the use and/or the diffusion of data are specific to some national legislations.

As an example it could be mentioned the so called right of reproduction of cultural goods that, according to the national laws of some countries (e.g., Italy), limits the possibility to reproduce cultural goods and diffuses such reproductions without the authorizations of certain public entities.

Depending on the relationship between the user of data and the entity the data refers to, other legal obligations, with different characteristics could arise from national legislations, such as the obligation not to violate unfair competition laws.

Finally, the person who reuses data should check that his reuse does not breach a contract he expressly entered into prohibiting such acts.

1.4.2 Statistical confidentiality and public security secrecy

Some data can not be communicated, spread and, more generally, reused. This exclusion is set up by national laws and Directive 2003/98/EU on the reuse of public sector information maintains it safe (Article 1, 2 (c))⁹⁶.

⁹⁶ The directive on the re-use of public sector information (Directive 2003/98/EC, known as the 'PSI Directive') provides a common legal framework for a European market for government-held data (public sector information). It is built around two key pillars of the internal market: transparency and fair competition.

The PSI directive was revised by Directive 2013/37/EU. The PSI directive focuses on the economic aspects of re-use of information rather than on the access of citizens to information, encouraging Member States to make as much information available for reuse as possible. It addresses material held by public sector bodies in the Member States, at national, regional and local levels, such as ministries, state agencies, municipalities, as well as organisations funded for the most part by or under the control of public authorities.

We refer to data that are excluded from access on the grounds of protection of national security (i.e. State security), defense, public security, or statistical confidentiality⁹⁷.

Those limitations entail data collected and stored by public sector bodies; accordingly, if someone wants to access and reuse that data he/she shall respect the exclusions avoiding any reuse of it.

Responsibilities, penalties and sanctions are imposed by national laws.

⁹⁷ Statistical confidentiality is a fundamental principle of European statistics. This field of statistics defines principles, concepts and procedures to keep data confidential while still permitting its use for statistical purposes.

EU Regulation 223/2009 on European Statistics defines it as *“the protection of confidential data related to single statistical units which are obtained directly for statistical purposes or indirectly from administrative or other sources and implying the prohibition of use for nonstatistical purposes of the data obtained and of their unlawful disclosure”* (Article 2, point c). In this context, ‘confidential data’ means *“data which allow statistical units to be identified, either directly or indirectly thereby disclosing individual information”*.

Individual data collected by statistical offices for statistical compilation, whether they refer to natural or legal persons, has to be strictly confidential and used exclusively for statistical purposes. Nonetheless, Regulation 223/2009 set up specific exceptions for scientific purposes (Article 23) and for the case where the statistical unit has unambiguously agreed to the disclosure of data (Article 20(3), point b).

2. Strategies, Measures, Technical Tools

This section will analyse how to set the DECODE technology in order to foster generation of digital commons.

Existing and already established tools will be examined, particularly, free licenses.

Moreover, new tools that could be used taking advantage of the characteristics of DECODE technology (particularly, the features that allow writing and adopting smart rules) will be examined.

Generally speaking, different scenarios will be considered and a precautionary rule will be adopted: if there is a potential problem and there is a measure easy to adopt to avoid such problem (even if it is simply potential), the safer strategy (adopt such measures) will be considered.

Further, measures that could foster the utility of the technology in allowing the processing of personal data in compliance with the EU privacy rules (the GDPR, etc.) will be analysed, such as providing documentation which can be useful to allow adopters of the technology to easily comply with their responsibility to document their compliance with such rules.

2.1 Different solutions for different ownerships

Ownership is a complex and polysemous legal category, that covers different legal domains and that has different meanings in different fields.

It has been developed within the property rights domain and then extended to copyright laws and other intellectual property rights (IPRs). In the last years data scientists - and generally the data literature - started to use it.

Nevertheless, using 'ownership' referring to the set of rights and powers of the natural person or entities "owning" rights on data regardless of the specific legal context is misleading and should be avoided.

The different concepts of data ownership that refer to the different legal domains are not interchangeable: each of the different 'ownerships' is characterized by different rules, rights conferred to the owner, exceptions etc., therefore a unified transdisciplinary concept of ownership is useless and even misleading; managing ownerships requires setting a list of different ownerships depending on the different legal fields (for example,

copyright ownership, performer's related right ownership, and ownership referred to personal data).

In conclusion, it is not possible to reduce to unity ownership on data and the most effective way to manage different ownerships seems to be dealing with the different 'ownership' in the legal fields adopting the strategies, tools and methods that better fit with each of that legal domains⁹⁸.

Accordingly, the previous sections of this document have identified different meanings of the term ownership applied to data.

For example, on a picture of the face of a natural person that is part of a dataset can coexist:

- the right of the photographer, or of the person or entity to whom the photographer assigned his rights on the picture;
- the rights (privacy rights and, depending on the circumstances, personality rights) of the natural person portrayed in the picture;
- the copyright and/or sui generis rights of the creator of the dataset.

This complexity is usually managed requiring provisions of disclaimers and warranties clearing rights on the data provided by one to another.

Rules on the exclusion of liability of the information service provider (see Section 1.1 of this document) interfere with this.

In short, the coexistence of different legal regimes requires to adopt a strategy to differentiate measures and tools to be adopted in order to clear each and all the rights related to the same data: licenses, information and consent to be provided according to privacy law, disclaimers and contractual clauses should be jointly managed by the DECODE technology (like they are by web service providers). Measures and tools should be determined depending on the circumstances and the role of the person or entity involved with the processing of data.

Analysing each legal framework separately and identifying the tools and measures required by that legal framework to clear the rights of the owner allows to manage the problem.

⁹⁸ A similar and useful analysis of data entitlements is conducted within DECODE in M.Al-Bassam ,S. Bano, G. Danezis, M. deVilliers, A. Sonnino (2017). Survey of Technologies for ABC, Entitlements and Blockchains.

2.2 Smart rules and smart contracts

A smart contract is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts were first envisioned by Nick Szabo in 1996.

He describes smart contracts as: “*New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts “smart”, because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises*”⁹⁹.

Proponents of smart contracts claim that many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both. The aim with smart contracts is both to provide stronger security than traditional contract law and to reduce other transaction costs associated with contracting.

Scholars debate whether smart contracts should be considered ‘contracts’ in the traditional legal meaning.

Some of them insist on the technological features of smart contracts. For example, according to Szabo, a smart contract is “*a computerized transaction protocol that executes the terms of a contract*”. What makes smart contracts “smart” is the underlying technology, that makes them essentially software programs running on a distributed ledger technology¹⁰⁰.

⁹⁹ N. Szabo, *Smart Contracts: Building Blocks for Digital Markets*, 1996, available here: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschoel2006/szabo.best.vwh.net/smart_contracts_2.html. See also, Felten E. (2017). *Smart Contracts: Neither Smart nor Contracts?*. In: *Freedom to Tinker: research and expert commentary on digital technologies in public life*. Available at <https://freedom-to-tinker.com/2017/02/20/smart-contracts-neither-smart-not-contracts/>

¹⁰⁰ N. Szabo, (1994). *Smart Contracts*. Available online: <http://szabo.best.vwh.net/smart.contracts.htm>.

The first, and most relevant, consequence is the *decentralization*: the DLT protocol runs on network of nodes, this way removing:

a) the need for a centralized platform, avoiding reliance on centralized authorities to mediate transaction;

b) the need for trust, thanks to sophisticated cryptography ensuring security and the reliability of the records appended onto the ledger, in form of blocks of code.

Smart contracts might serve, thanks to their nature of self-executing agreement, as a tool to remove socioeconomic barriers that keep the relatively disadvantaged from attaining their legal due, by distributing enforcement outside the centralized court system.

Others focus on the mutual promises embedded into technology. This is the case of Glatz, who defines smart contract as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises”¹⁰¹.

The point is controversial and refers to what ‘contract’ means.

A contract in the traditional sense is an agreement between two or more parties to do or not to do something in exchange for something else, where mutual assent must be manifested by making a promise and/or rendering performance, and it may be written or spoken.

Then, some scholars state that “if intent cannot even implicitly be detected between the parties (if there are any), the smart contract does not constitute a contract with legal effects and is rather no more than a computer program built into the blockchain”¹⁰².

Anyway, according to various authors “a smart contract is not an agreement, per se. Nonetheless, a smart contract may be some kind of evidence for an agreement, or may be a means for the execution of provisions of a contract”¹⁰³.

It is important to stress that some fundamental issues of contract law are difficult to instantiate in code. This is the case, for example, of “issues dealing with temporality (such as mutual mistake in setting forth contract terms, or rescission), or standards that

¹⁰¹ See F. Glatz (2014). What are Smart Contracts? In search of a consensus. Available online at: <https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad>. Where:

a set of promises refers to the (often mutual) rights and obligations to which the parties of a contract consent. Those promises define the nature and purpose of the contract; and ‘digital form’ means that the contract has to be written in machine-readable code. This is necessary because the rights and obligations established through the smart contract are executed by a computer or a network of computers as soon as the parties have come to an agreement.

To specify this further:

(1) coming to an agreement

When do the parties of a smart contract come an agreement? The answer depends on the specific smart contract implementation. Generally-speaking, an agreement is found (at the latest) when the parties have committed themselves (irrevocably so) to the execution of the contract by installing the contract on a contract host platform.

(2) contract execution

What “execution” really means is as well implementation-dependent. Generally-speaking, execution means pro-active enforcement mediated by technological means.

(3) machine-readable code

Furthermore, the specific “digital form” the contract needs to be drafted in depends heavily on the choice of protocols which the parties agree to use.

¹⁰² Lauslahti, K., Mattila, J., Seppälä, T. (2017). *Smart Contracts – How will Blockchain Technology Affect Contractual Practices* ? ETLA Reports (Vol. 68, pp. 1–26), p. 21.

¹⁰³ Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A. B., Weber, I., Xu, X., Zhu, J., (2017). Risks and opportunities for systems using blockchain and smart contracts. Data61 (CSIRO), Sydney, p. 33.

apply to contracts and contractors across the board, even if not represented on the fact of the document (such as the duty of good faith)”¹⁰⁴.

Moreover, in order to be legally enforceable, the contract must fulfill the conditions imposed by law, such as two or more parties, the capacity of the parties, and mutual assent, based on the concepts of offer and acceptance by the parties to the contract.

One of the main features of smart contracts, which remarkably distinguishes them from traditional ones, is that they can be fully automated and self-enforcing: once the terms and conditions are set in computer code, they will be executed impartially by the computer, on the basis of the code and the exogenous events. This is opposed to the way in which traditional contracts are enforced and the enforcement phase formally depends on centralized institutions - the courts - to set disputes.

Then, the notion and the legal meaning of smart contracts is still unclear and this may diminish trust. This is the reason why in the context of the DECODE Project, the concept of ‘smart rules’ , rather than ‘smart contracts’ , should be emphasised.

In this context, smart rules:

- are a set of algorithmic protocols expressed in a formal language that implement flexibility in control data sharing. Smart rules could be used to define what data is accessible and reusable, how data should be managed in terms of access, value attribution and other parameters, and legal/contractual obligations and other constraints;
- follow a defined ontology to define access to subsets of data (e.g., personal data or for specific uses granted to specific subjects);
- can also be used to revoke authorisation for access or change the legal status and the conditions of use and exploitation of the data.

Those smart rules “*can be expressed in a declarative language, which is then compiled in a functional language and executed.*

Smart rules enable providers and app developers to define rules about operation of the system or the regulatory environment. Such abstraction between people’s choices and its enforcement creates a rich landscape for flexible and decentralised creation of new applications and services”¹⁰⁵.

Therefore, the definition of smart rules adopted within DECODE goes beyond automatic self-enforcement and includes contractual obligations. The smart rule definition adopted within the DECODE Project aligns with the definition of Ricardian contract adopted by Ian Grigg in his paper “Ricardian contract” (Grigg, 2004): “A *Ricardian*

¹⁰⁴ Levy, K. E. C. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science, Technology, and Society*, 3, 1, p. 4. <https://doi.org/10.17351/ests2017.107>.

¹⁰⁵ See S. Bano, E. Bassi, M. Ciurcina, A. Freire, S. Hajian, J.-H. Hoepman (2017). Privacy by Design Strategies for DECODE Architecture.

*contract can be defined as a single document that is a) a contract offered by an issuer to holders, b) for a valuable right held by holders, and managed by the issuer, c) easily readable (like a contract on paper), d) readable by programs (parsable like a database), e) digitally signed, f) carrying the keys and server information, and g) allied with a unique and secure identifier*¹⁰⁶.

DECODE Smart Rules allow the conclusion of legally binding agreements between the users, and, therefore, the creation of legal obligations.

This opens the way for the DECODE pilots (but also for other users of the DECODE technology) to implement specific Smart Rules that permit to achieve a wide range of goals, including the goals pursued by the DECODE Project, aiming at:

- *"Creating a framework in which people want to share their data in a controlled way for the common good,*
- *Finding technological solutions that enable the enforcement of rules for data sharing, preventing the misuse of data,*
- *Testing whether there are viable alternative revenue generation models in an internet economy which finances itself predominantly through monetising personal data,*
- *Finding the right way to govern decentralised digital platforms so that contributors have a genuine stake and say in how they are run*¹⁰⁷.

2.3 Free licenses for DECODE

This section dwells on how intellectual property rights may affect the development and use of the DECODE technology. The aim is to flash out which free licenses may let DECODE meet the needs of the communities involved.

2.3.1 Free licenses for the DECODE technology

DECODE technology will be composed of software to be deployed in the DECODE OS and DECODE Nodes.

¹⁰⁶ See http://iang.org/papers/ricardian_contract.html

¹⁰⁷ See Deliverable 1.7 "Project methodology and policy review", p. 10.

Adopting free software licenses (with preference with copyleft licenses) for such software is certainly a suitable strategy to meet the needs of the communities involved with its development and use.

Moreover, licensing of all the software developed within the project under the terms of free software licenses is also required by the Consortium Agreement signed by (and therefore binding on) the partners of the project.

Particularly, section 9.8.3 of the Consortium Agreement states that *“The parties agree to publish and distribute Results that constitute Software under a “DECODE Accepted Software License”. Any proposal to disseminate and/or distribute Software under a license that is not a “DECODE Accepted Software License” shall be subject to the approval of the General Assembly. To the extent possible, the General Assembly shall determine the DECODE Accepted Software License applicable to each element of Results as soon as possible within the development process so as to achieve orderly management of IP and Software in the project and with the goal of maximizing the adoption of the Software by users and the availability for users of the Source Code of the Software and of Derivative Works of the Software”.*

Section 9.8.1 states that *““DECODE Accepted Software License” means any Free Software Licence, with a preference towards GPL, LGPL and AGPL”.*

Thus, a preference towards the copyleft licenses published by the Free Software Foundation is set: this is in line with the ethos of the free software communities.

The DECODE technology could be developed reusing existing free software. Therefore, the license terms of reused software shall be respected. If programs are released under a copyleft license, it follows that licensing options for the code developed within the project should be taken for granted.

It is therefore useful to adopt policies to comply with the license obligations of the software reused.

For this purpose, it may be useful to follow a specification, in order to properly comply with the requirements of free software licenses, such as the OpenChain specification¹⁰⁸, published by the OpenChain Project and endorsed by the Linux Foundation.

Patent issues have also to be considered.

It is therefore useful to conduct enquiries to check that the software developed or reused within the DECODE technology does not interfere with patent rights hindering its use.

Even if it is not possible to be sure that patent rights do not exist, reasonable efforts should be devoted to such inquiries to minimize any risk of litigation.

¹⁰⁸ See <https://www.openchainproject.org/>

DECODE technology could trigger the development of other artifacts besides software (e.g., graphical elements of user interfaces, ontologies, integrated circuits of the devices, shape of the devices): such artifacts should require the adoption of adequate licensing strategies to allow the use, modification and distribution, including in modified form, of the artifacts, meeting the practical and ethical needs of the communities involved.

2.3.2 Free licenses for the data shared with DECODE

Datasets resulting from the use of the DECODE technology could be subject to copyright or *sui generis* right on databases.

Moreover, depending on the circumstances, the contents of the above datasets could be subject to copyright, related rights and other rights (such as trade secret rights, and personality rights): usually, this issue is addressed by requiring the data providers a disclaimer in order to smooth out the responsibility of the data recipient.

Adoption of tools that allow to license the datasets generated by the use of the technology is recommended to properly manage copyright and *sui generis* right on databases and copyrights and related rights on the content of such datasets.

In order to allow third parties to the use of datasets generated by the use of the technology, adoption of free licenses is advisable.

Adoption of free licenses will not interfere with the privacy rights of the interested persons if such datasets include personal data.

The rights of the data subjects need to be dealt with different ways, adopting different legal tools, as it will be explained in the next section.

2.4 Legal rules and technical strategies for privacy and data protection compliance

In this section we analyse the strategies and rules to adopt for privacy and data protection compliance within DECODE.

We distinguish between rules and strategies for the DECODE OS technology and rules and strategies for data services that will adopt the DECODE technology.

In the first case (2.4.1), rules and strategies are addressed to the developers and producers of DECODE OS technology. In the second one (2.4.2), they are addressed to

the subjects that will organize services based on DECODE OS technology who that will act with the powers and responsibilities of data controllers and/or data processors.

2.4.1 Legal rules and technical strategies for privacy and data protection compliance of DECODE OS

It is important that the DECODE technology will be designed and developed in a way that is compliant with privacy and data protection laws. This is crucial for different reasons.

First of all, the compliance with laws protecting privacy rights can foster trust in the use of DECODE technology and in the possibilities that it offers to citizens, communities and city administrations.

The DECODE technology aims to be adopted for services as wide as possible, without barriers to the eventual processing of personal data.

Moreover, the DECODE technology shall be designed in a way that ensures the protection of privacy and personal data rights for the natural persons involved.

Here follows a first list of the main rules from the GDPR the DECODE data controller(s) shall be compliant with:

- adopting adequate means to ensure the security of the data processing (Article 32);
- ensuring data integrity (Article 5(1), point f);
- providing a technology for certified data access (Article 5(1), point f);
- adopting pseudonymisation techniques and encryption as default measures (Articles 25(1) and 32(1), point a);
- ensuring and maintaining the complete traceability of data processing (Article 30);
- taking adequate measures to ensure data subjects rights according to GDPR Articles 15-22 (Article 12);
- adopting adequate tools for ensuring the right to revoke the consent to personal data processing, in a way that data are no longer processable (according to Article 7);
- adopting adequate tools for ensuring the right to erasure of the data subject (Article 17).

Here we list some strategies to adopt for data protection compliance:

- providing the DECODE OS technology with a complete risks assessment (and publishing it) with the aim to increase transparency and thereby fostering trust;
- specifying and adopting privacy by design measures;
- providing smart rules and smart contracts that allow to define roles, activities and

responsibilities of the different entities who, directly or indirectly, process personal data with DECODE OS technology.

2.4.2 Legal rules and technical strategies for privacy and data protection compliance of data processing within services based on DECODE technology

When an entity decides to adopt the DECODE technology to provide a service, some responsibilities descend. Among them, if the service includes processing of personal data, responsibility to comply with data protection rules follows as a result.

Responsibilities to be compliant with privacy and data protection laws are pending on who determines means and purposes of the personal data processing becoming the data controller.

We recall here the responsibilities of the data controller (see *supra* 1.3.1.4).

Data controllers have to comply with the following obligations provided by the GDPR:

- collecting consent by the data subjects (Article 6(1), point a) unless other legal bases for lawful processing apply;
- providing information to the data subjects in order to assure the data subject's rights (Articles 12-14);
- keeping the necessary actions in order to assure the exercise of the data subject's rights under Articles 15 to 22; in particular allowing data rectification and erasure (Article 16 and 17);
- adopting privacy by design and privacy by default measures (Article 25);
- keeping record of processing operations (Article 30);
- adopting security measures (Article 32);
- providing notification of a personal data breach to the supervisory authority and communication of the data breach to the data subject (Articles 33 and 34);
- providing a Privacy Impact Assessment (PIA) where it is necessary (Article 35);
- designate a Data protection Officer (DPO) where it is necessary (Article 37).

It is also important to remind the legal limitations concerning the sharing data (see *supra* 1.4, 1.4.1 and 1.4.2). Against this backdrop, the data controller shall specify the data to be processed, in accordance with the following principles:

- the purpose limitation principle,
- the minimization principle,
- the storage limitation principle and
- the adoption of pseudonymisation and encryption as default measures.

Particular attention has to be devoted to the use, within DECODE, of distributed ledger technologies (DLT) allowing use of smart rules (SR).

This poses risks and opportunities if personal data are to be processed through such DLT and SR.

At the stage of the DECODE project, this possibility is not excluded according to the results of the Tech Symposium of DECODE project that took place on 20th & 21st September 2017 in London, where, concerning Chainspace - the DLT to be possibly adopted within the project -, it was stated that *“Chainspace is a public blockchain implementation, therefore no personally identifying data can be stored within Chainspace”*.

We remind that personal data is data referring to an identified or identifiable natural person. Personal data could consist in identifying data (e.g. name, address, identification number) and not identifying data (e.g. age, gender). So, we cannot exclude that within the DLT to be adopted within DECODE technology personal data processing will take place.

Here we examine the different entities who operate within the DECODE context on the basis of their activities and of their roles under the conceptual frame provided by the GDPR.

This analysis will make easier to stress the possibility to process personal data lawfully within services based on DLT.

It is possible to identify the following roles within DLT to be adopted within DECODE technology:

DLD (DL Developer)= who develops and licenses the software that allows the DLT to run;

DLS (DL Storer) = who runs the software that allows the DLT to run and stores the DLT;

SRC (SR Creator) = who publishes on the DLT a SR (model) that can be used by different parties but he is not a SRDP, SRDR, or DLSC;

SRDP (SR Data Provider) = SR party that provides his personal data;

SRDR (SR Data Recipient) = SR party that gets access to personal data to use it (becoming data controller);

DLSC (DL Service Controller) = entity who determines the objectives and the purposes of a service and the adoption of DLT and SR for its realization.

In the following table we map the above roles with those provided by the GDPR and suggest possible strategies to foster adoption of DLT and SR by the subjects involved in the use of the DECODE technology.

Role in DLT	Possible roles according to GDPR	Strategies
DLD	technology provider	Limit DLD responsibility by not taking decisions concerning purposes and means of data processing
DLS	data controller / data processor	Allow DLS to enter into an agreement with data controllers stating its role of data processor (according to art. 28(3) of GDPR) to limit its responsibility
SRC	technology provider	Limit SRC responsibility by not taking decisions concerning purposes and means of data processing
SRDP	data subject	Make available Terms of Service not designed by (and in the interest of) the DLSC
SRDR	data controller	Allow SRDR to comply with GDPR
DLSC	data controller / data processor	Allow DLSC to comply with GDPR and to be aware of the risks depending on the adoption of the DECODE DLT

If a DLT includes SR designed to clearly define the respective roles, duties and responsibilities among parties mentioned above, it would be easier for SRDR and DLSC (data controllers) and for DLS (data processor) to adopt such DLT.

Finally, in the interest of the SRDP, especially when they are natural persons / citizens, it would be interesting to design SR that are not unbalanced in favour of the SRDR and DLSC, but that allow the data subject (SRDP) to 'personalize' options for personal data sharing

For example, it could possible to include in SR a law clause allowing a more favourable legislation for natural persons and citizens, such as the EU legislation, upon which consent will be given at the time the participants join the service based on the DECODE technology.

3. Legal guidelines for the development of the DECODE OS

This section aims at providing practical support to the technical work to be performed within DECODE with the goal of complying with law and fostering creation of digital commons.

On one side, it will list the recommendations deriving from the legal analysis performed above (4.1)

On the other side, it will propose a domain taxonomy (4.2) to support the design of the ontologies to be adopted within the project for the implementation of the DECODE technology.

3.1 Recommendations

This section distinguishes recommendations in:

- recommendations on the design of the DECODE OS (3.1.1), and
- recommendations on the design of the Smart Rules syntax (3.1.2).

3.1.1 Recommendations on the design of DECODE OS

1) Recommendation on Licensing:

a) Developing the **software** included in the DECODE OS, adopt policies for:

- managing copyright issues (as way of example, following the OpenChain specification);
- using reasonable effort to verify that no patents interfere with the use of DECODE OS;
- adopting free software licenses for all the components of the technology.

- b)** In the design of the **artifacts not consisting in software** included in the DECODE OS:
- adopting licenses that allow use, modification and distribution, including in modified form, of the artifacts.

2) Recommendation on Data Protection Compliance:

a) Design the DECODE OS in a way that it allows compliance with GDPR obligations, including:

- the safeguard of the data subject's rights (e.g. the right to erasure, that shall be performed by the data controller) (Articles 15 to 22);
- the adoption of privacy by design and privacy by default measures (e.g. pseudonymisation by default) (Article 25);
- keeping record of the processing operations (Article 30);
- the adoption of measures to assure the security of data processing (Article 32).

b) Release the DECODE OS in bundle with:

- documentation that allows the users to easily perform a Privacy Impact Assessment (according to Article 35 of GDPR);
- documentation providing a risks evaluation (according to Article 32 of GDPR), that could be automatically included in the PIA adopted by the data controller of the service.

3.1.2 Recommendations on the design of smart rules syntax

1) Smart rules should allow:

- each party to receive notice of the offer and/or acceptance or their revocation by the other party/ies;
- to include statements (such as clauses, disclaimers or licenses that are part or not of the document);
- to express offer and/or acceptance to the whole document;
- to express disjoint offers and/or acceptances to specific statements included or related to the document;
- to revoke expressed offers and/or acceptances to specific statements (as way of example: consent revocation)
- to include explicitly and in a clear language licensing rules for data.

2) If the smart rules concern personal data processing:

- they shall use an intelligible and easily accessible form, using clear and plain language (according to Article 7(2) of GDPR);
- the data subject should be allowed to provide an informed consent (according to Articles 6 and 4(1), point 11, of GDPR);
- the data controllers should be allowed to provide information on the personal data processing (according to Articles 13 and 14 of GDPR);
- data processor(s) should be allowed to enter into a contract or other legal act with data controller(s) (according to Article 28 of GDPR);
- joint controllers should be allowed to enter into an arrangement between them and to make available the essence of such arrangement to the data subjects (according to Article 26 of GDPR).

3.2 Legal domain taxonomy

Annex B of this document offers a legal taxonomy for the DECODE project. On the one hand, it supports the design of the ontologies to be adopted within the project for the implementation of the DECODE technology. On the second hand, it provides the reader with the conceptual tools to understand the key notions of the different legal fields relevant for the DECODE project.

4. References

We attach **Annex C** to this document.

Annex C is a first bibliography of the legal domains involved by DLT and relevant for DECODE Project.

Here follows the list of references of this document.

Al-Bassam, M., Bano, S., Danezis, G., deVilliers, M., Sonnino, A. (2017). Survey of Technologies for ABC, Entitlements and Blockchains

Bain, Malcom. "Software Interactions and the GNU General Public License" *International Free and Open Source Software Law Review*, 2-2 (2010). Accessed June 15, 2017. <http://www.ifosslr.org/ifosslr/article/view/44>

Bano S., Bassi E., Ciurcina M., Freire A., Hajian S., Hoepman J.-H. (2017). Privacy by Design Strategies for DECODE Architecture

Bass, T., Symons, T., (2017), Project methodology and policy review

Berberich M., Steiner M. (2016). Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?. *EDPL* (3), pp. 422-426

Cavoukian A. (2010). Privacy by Design: the definitive workshop. In *Identity in the information society* (3) 2, pp. 247-251

Colesky M., Hoepman J.-H., Hillen C. (2016). A critical analysis of Privacy Design Strategies, 2016 IEEE Security and Privacy Workshops, pp. 33-40

De Filippi P. (2016). The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies. *Journal of Peer Production*, Issue n.7: Alternative Internets. Available at SSRN: <https://ssrn.com/abstract=2852689>

Elliott, Mark. "Stigmergic Collaboration: The Evolution of Group Work" *M/C Journal*, 9-2 (2006). Accessed October 10, 2017. <http://journal.media-culture.org.au/0605/03-elliott.php>

Felten E. (2017). Smart Contracts: Neither Smart nor Contracts?. In: *Freedom to Tinker: research and expert commentary on digital technologies in public life*. Available at <https://freedom-to-tinker.com/2017/02/20/smart-contracts-neither-smart-not-contracts/>

Floridi L. (2016). Four challenges for a theory of informational privacy. In *Ethics and Information Technology* (8) 3 pp. 109-119

Fontana, Richard, and Kuhn, Bradley M., and Moglen, Eben, and Norwood, Matthew, and Ravicher, Daniel B., and Sandler, Karen, and Vasile, James, and Williamson, Aaron. A Legal Issues Primer for Open Source and Free Software Projects, Accessed May 16, 2017. <http://softwarefreedom.org/resources/2008/foss-primer.pdf>

Fuster Morell M. (2010). *Dissertation: Governance of online creation communities: Provision of infrastructure for the building of digital commons*

Glatz F. (2014). What are Smart Contracts? In search of a consensus. Available online at: <https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad>

Grigg, Ian. The Ricardian Contract. In Proceedings of the First IEEE International Workshop on Electronic Contracting, pages 25-31. IEEE, 2004. http://iang.org/papers/ricardian_contract.html

Hardin G. (1968), *The tragedy of the Commons*. Science, vol. 162, N. 3859, pp. 1243-1248

Hemel, Armijn, and Coughlan, Shane. Practical GPL Compliance. San Francisco, CA: Linux Foundation, 2017

Hess C., Ostrom E. (2007). *Understanding Knowledge as a Commons: From Theory to Practice*. The MIT Press: Cambridge, MA

Himanen P.(2001), *The hacker ethic and the spirit of the information age*, Random House

Hoepman, J-H. (2014). Privacy Design Strategies, IFIP TC11 29th Int. Conf. on Information Security (IFIP SEC 2014), pp. 446-459

Koops B-J., Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law'. In: *International Review of Law, Computers & Technology* (28), 2, pp. 159-171

Kuhn, B. M., Sebro, A. K. Jr., Gingerich, Denver, and Free Software Foundation, Inc., and Software Freedom Law Center. *Copyleft and the GNU General Public License: A Comprehensive Tutorial and Guide*, Accessed May 16, 2017. <https://copyleft.org/guide/>

Lauslahti K., Mattila J., Seppälä T. (2017). *Smart Contracts – How will Blockchain Technology Affect Contractual Practices ?* ETLA Reports (68), pp. 1–26

Levy K. E. C. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science, Technology, and Society*, (3) 1, Available online at. <https://doi.org/10.17351/ests2017.107>

Margoni, Thomas. "Not for Designers: On the Inadequacies of EU Design Law and How to Fix It" *Journal of Intellectual Property, Information Technology and E-Commerce Law*,

4-3 (2013). 225-248. Accessed May 16, 2017. <http://www.jipitec.eu/issues/jipitec-4-3-2013/3845/margoni.pdf>

Meeker, Heather, *Open source for business. A practical guide to open source licensing*. North Charleston SC: Createspace Independent Publishing Platform, 2017

Metzger, Axel. *Free and Open Source Software (FOSS) and other Alternative License Models: A Comparative Analysis*. Switzerland: Springer International, 2016

Ostrom E. (1990), *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press

Paccagnella L. (2007). Robert Merton e il software libero: gli imperativi istituzionali della ricerca scientifica nell'etica hacker. In: *Quaderni di Sociologia*, 45, pp. 163-178

Pagallo, U. (2012). On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In Gutwirth S., Leenes R., De Hert P., *European Data Protection: In Good Health?*. pp. 331 – 346

Peeters R., Pulls T. (2015). *Regaining the end-users' trust with transparency-enhancing tools*. In Amsterdam Privacy Conference 2015

Rosen, Lawrence. *Open source licensing: software freedom and intellectual property law*. Upper Saddle River, NJ: Prentice Hall Professional Technical Reference, 2005

Rouvroy A., Poullet Y. (2009), The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) *Reinventing Data Protection?*. Springer, Dordrecht

Staples M., Chen S., Falamaki S., Ponomarev A., Rimba P., Tran A. B., Weber I., Xu X., Zhu J., (2017). Risks and opportunities for systems using blockchain and smart contracts. Data61 (CSIRO), Sydney

Szabo N., (1994). Smart Contracts. Available online: <http://szabo.best.vwh.net/smart.contracts.htm>

Szabo N., Smart Contracts: Building Blocks for Digital Markets, 1996, available here: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.htm

Van den Brande Y., et Al.. *The International Free and Open Source Software Law Book*. Open Source Press GmbH, 2011. Accessed May 16, 2017. <http://ifosslawbook.org/>

Weber, Steven. *The Success of Open Source*. Cambridge, Massachusetts: Harvard University, 2004

Zyskind G., Nathan O., Pentland A. (2015). Decentralizing privacy: Using blockchain to protect personal data. Security and Privacy Workshops (SPW), 2015 IEEE

Annex A: Notes for a definition of Digital Commons

by CNRS¹⁰⁹

1. Digital commons definition

In the field of legal sciences, each notion that regulates relevant aspects of social life requires that the object of the norm is well defined. The definition of "digital commons" has been discussed by scholars and social activists. Their backgrounds are characterized by significant differences, depending on their cultural context and areas of scientific interest.

In order to define digital commons, we have to consider two main research fields:

1. the first follows by the work of Elinor Ostrom and her pupils;
2. the other one relates to the debate inside the free software movement.

Consequently, we will try to show how the problem to define digital commons may be brought back two largely independent theoretical approaches.

In the Ostromian perspective, the institutional features that characterize commons are rethought after the effects of technological progress. Indeed, the digital-related aspects represent a new research frontier within the commons topic.

In the second case we find the opposite: the institutional issue raises only in a second moment; particularly, the free software movement recognizes the importance of the social cooperation that is necessary for the production of the free software, but it does not focus on the relevance of the formal institutions. The institutional problem is mainly reduced to a set of practices aiming at the free software safeguard. In other words, the free-software movement focuses on the defence of individual freedoms and the denial of proprietary principles without however bothering to build norms or conventions similar to those identified and partly formalized by Elinor Ostrom. The following two paragraphs are aimed to present and discuss how digital commons are defined in both the Ostromian perspective and the free software movement's view.

¹⁰⁹ Annex A was written by Stefano Lucarelli, Elena Musolino, Giulia Rocchi and Riccardo Gherardi.

1.1 From knowledge commons to digital commons. The Ostromian perspective and beyond

In their introduction of "*Understanding Knowledge as a Commons*"¹¹⁰, Ostrom and Hess make just a brief reference to the risks that new digital technologies can produce in terms of new restrictions on users' freedom. In 2006, when the book was published, digital technologies were at a very early stage.

Nevertheless, Ostrom and Hesse expressed the urgency for an authentic common good "culture" in order to contrast new forms of enclosures and to protect collective access to knowledge as a fundamental right of the person. As a matter of fact, they already suggested some potential solutions to the problems connected to the exploitation of digital resources. For example, they focused on identifying how to preserve and make digital content available on the Web: Open Content, Creative Commons and Open Source are the main solutions the authors suggest in order to ensure a democratic worldwide access to knowledge.

It is undeniable that the theoretical path followed by Ostrom and her pupils, starting from natural commons, goes toward the concept of digital commons, conceived as a subset of knowledge commons.

In other words, Ostrom's perspective tends to underestimate how technological progress can affect the characteristics of commons identified in the 1990 book ("*Governing the Commons*"¹¹¹), which we'll briefly illustrate below.

As well known, the purpose by Ostrom is dismantling Garrett Hardin's thesis, a still today "die hard" argument¹¹². In Hardin's opinion, commons would not represent a durable management model: their sustainability would entail their privatization, or the use of the so-called bureaucratic Leviathan, id est an extremely invasive public intervention.

Ostrom - unlike Hardin's use of the abstract example of Foster pasture as the basis of his reasoning - travelled around the world to collect stories, data and long-standing commons experiences. From this backdrop, she suggested a notion of "

users' common pool resources (CPR) self-management", rich of political path. After comparing all the cases she studied, Ostrom identified a set of necessary design principles that can be traced back to long-enduring institutions that are responsible for CPR' management, principles shared by all successful stories:

¹¹⁰ Hess C., and Ostrom E. (2007). *Understanding Knowledge as a Commons: From Theory to Practice*. The MIT Press: Cambridge, MA.

¹¹¹ Ostrom E. (1990), *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press.

¹¹² Hardin G. (1968), *The tragedy of the Commons*. Science, vol. 162, N. 3859, pp. 1243-1248.

Table 1: Design principles illustrated by long-enduring CPR institutions¹¹³

1	<p>Clearly defined boundaries</p> <p>Individuals or households who have rights to withdraw resource units from the CPR must be clearly defined, as must the boundaries of the CPR itself.</p>
2	<p>Congruence between appropriation and supply rules, as well as with local conditions</p> <p>Appropriation rules restrict time, location, technology, and/or quantity of resource units are related to local conditions and to provision rules requiring labour, material, and/or money.</p>
3	<p>Collective-choice arrangements</p> <p>Most individuals affected by the operational rules can participate in modifying the operational rules.</p>
4	<p>Monitoring</p> <p>Monitors, who actively audit CPR conditions and appropriator behaviour, are accountable to the appropriators or are the appropriators.</p>
5	<p>Graduated sanctions</p> <p>Appropriators who violate operative rules are likely to be gradually assessed by sanctions (depending on the seriousness and context of the offense) by other appropriators, by officials accountable to these appropriators, or by both.</p>
6	<p>Conflict-resolution mechanisms</p> <p>Appropriators and their officials have access to low cost local arenas to resolve conflict among appropriators or between appropriators and officials.</p>

¹¹³ Ostrom E. (1990), *ibidem*, p. 90.

7	<p>Minimal recognition of rights to organize</p> <p>The rights of appropriators to devise their own institutions are not challenged by external governmental authorities.</p>
8	<p><i>For CPR systems that are part of larger systems</i></p> <p>Nested enterprises</p> <p>Appropriation, provision, monitoring, enforcement, conflict resolution, and governance activities are organized in multiple layers of nested enterprises.</p>

The definition of a set of precise design principles such as those identified for natural resources proposed by Ostrom results not easy to, applied to digital commons; the same problem has been highlighted for commons related to knowledge. The main difficulty associated with this type of goods is that it is much more complicated to clearly define boundaries and limits for the use of resources that are no longer exhaustible such as in the case of natural commons: if access to a grazing land could be regulated by setting up times and ways of using it within the community, the same cannot be generally done with digital common goods. Digital resources can in fact be continuously exploited without affecting their use by other parties (not rivalry): in this sense, the rules to be applied for their efficient management at the community level need to be reformulated and adapted to the various features that these resources present. However, once accepted the difference due to the features of the considered resources, it is reasonable to extend Ostrom design principles not only to knowledge commons, but also to digital commons. The presence of collective decision-making methods, the definition of self-determined rules and sanctions for their violations, the application of methods of control and resolution of the conflicts, and the recognition to the participants of the right to organize themselves, are all principles that can be applied to the complex world of digital commons as well. To demonstrate this, in the following table the design principles identified by Ostrom are adapted to the case of free-software practices, showing that the possibility to achieve a communal organization of the digital commons is far from a utopian solution:

Tab.2 Ostrom's design principles adapted to the free software.

	OSTROM'S DESIGN PRINCIPLES	ADAPTATION TO FREE SOFTWARE
1	Clearly defined boundaries	The boundaries of a free-software project are defined by the lines of the code and the license.
2	Congruence between appropriation and supply rules, as well as with local conditions	The problem in this case is different because software does not allow exclusive use. In addition, there are different issues that could impact on appropriation and supply.
3	Collective-choice arrangements	Some projects adopt institutional entities to allow the governance of the project. The more a project is important, the more an entity governs its development.
4	Monitoring	Everybody is a potential supervisor, since the code is open.
5	Graduated sanctions	Free software licenses provide for mechanisms that provide for sanctions (with different degrees of progressiveness).
6	Conflict-resolution mechanisms	There are different no-profit service providers to support enforcement.
7	Minimal recognition of rights to organize	In free software this right is not minimal: everybody can fork the project and/or reuse the code.
8	Nested enterprises	This last point is different in free software.

From the comparison shown in the previous table, it seems reasonable to extend to the free software (and, in general, to the digital commons) the clear definition of

boundaries, the role of control and progressive sanctions, and also the recognition of the rights to self-organize. However, the congruence between ownership rules, supply and local conditions and the existence of methods of collective decision are more ambiguous than in the case of natural commons: the reason is given by the huge difference between these two categories of resources. Finally, the last principle, which underlines the necessity to have a structure based on several levels for larger communities, seems to be not particularly significant in relation to digital resources because these resources should not present problems of exploitation such as in the case of natural resources.

Ostrom and Hess themselves identified digital resources, which at that time were only making their appearance (and that had not shown their current enormous potential), as the natural evolution of common goods of knowledge. Ostrom and Hesse stated that¹¹⁴: “Commons can be strictly delimited (in the case of a public park or a library), they can cross boundaries and confines (Danube river, migrant animals, Internet), otherwise they can be without delimited border (Knowledge, stratum of ozone)”. As well, the fundamental requirement of a “public good” was its non-rivalry and the high cost of exclusion, characteristics that can be well applied to any work of the intellect, including the digital commons. In this sense, it can be reasonably stated that technological progress has changed the forms of knowledge (for example, consider the huge change occurred between material backdrops, such as a paper book, and modern online resources) but not the nature of knowledge itself. What has changed significantly if compared to a decade ago is the complexity and vastness that the phenomenon has achieved, but the principles underlying Ostrom and Hess's proposals remain valid in the message they wanted to promote: the logic of collective management, based on clear and self-imposed rules by a community of participating actors, remains valid and must only be modeled according to the different contexts in which it is applied.

¹¹⁴ Hess C., and Ostrom E. (2007). *Understanding Knowledge as a Commons: From Theory to Practice*. The MIT Press: Cambridge, MA.

1.2 New digital rights for a new technological paradigm: the digital commons in the perspective of the free software movement

Free software is a «total social phenomenon» in contemporary information society. As stressed by different scholars¹¹⁵, the model of production and diffusion of free software incorporates basic principles that have influenced modern western science. Free software leads to reconsider the institutional norms presented in the Robert K. Merton's famous essay of 1942: universalism, communism, disinterestedness and organised scepticism. The same norms perfectly depict the processes of production and diffusion of free software. More precisely, work autonomy, promotion of an active relationship with technologies and defence of free circulation of information represent values that have been embodied, constructed and consolidated in a constant to-and-for with free software community's practices: writing code, writing licenses, organizing collaborative work, campaigning against legislative texts.

It is evident that the declared intention to globally spread the ethos of the free software communities brings about an essential query: how to find institutional structures alternative to those implemented within proprietary regimes' logics? In some respects, these are new issues, if related to the specific community of the free-software movement. From a politically point of view, this community aims at the recognition of individual freedoms, but tend to neglect the claims aimed at defining new "collective choice-driven" institutions.

In conclusion: free software projects cannot be entirely considered as digital commons. As a matter of fact, writing a code and publishing it with a free license are not sufficient conditions in order to realize a free software. There are other necessary conditions, among them:

1. the reputation inside the community;
2. the adoption of the good practices diffused in the community (for instance public repository, continuous free upgrading, an efficient system of bugtrack and feedback ...);

¹¹⁵ Pekka Himanen, *The hacker ethic and the spirit of the information age*, Random House, 2001; Luciano Paccagnella, "Robert Merton e il software libero: gli imperativi istituzionali della ricerca scientifica nell'etica hacker", *Quaderni di Sociologia*, 45, 2007, pp. 163-178.

3. the quality of the code, including its documentation to allow understanding of the code;
4. the software's coverage, as the presence of automatic tests for evaluating the absence of bug on high percentages in the written code.

1.3 Towards a practical definition of Digital Commons

It should be stressed that digital commons, as the open and shared development of many digital resources that would otherwise be excluded to many, developed in opposition to the profit-oriented exploitation of digital resources.

«The digital commons are a form of commons involving the distribution and communal ownership of informational resources and technology. Resources are typically designed to be used by the community by which they are created»¹¹⁶. In particular, «The distinction between digital commons and other digital resources is that the community of people building them can intervene in the governing of their interaction processes and of their shared resources»¹¹⁷.

It follows that the key aspect of digital commons consists in the collective management by the community's participants: through this organizational mode, a community decides to collectively regulate the use of a resource, favouring fair access and sustainable use of the resource. The aim is to prevent that resources, in the case of digital commons resources, could be subject to restrictions that preclude or restrict access to many subjects who should have guaranteed the possibility to use them. Essentially, the risk to be avoided is that these restrictions become a modern form of enclosures that Ostrom described in "Governing the commons" in some local contexts regarding natural resources. Therefore, in order to facilitate an efficient regulation of digital resources, which is able to grant the widest access to these resources and avoid

¹¹⁶ Stadler F. (2010), *Digital commons: a dictionary entry*.

¹¹⁷ Fuster Morell, M. (2010), *Dissertation: Governance of online creation communities: Provision of infrastructure for the building of digital commons*, p. 5.

them being managed only by few private individuals¹¹⁸, movements in favour of digital commons want to promote access to them as a fundamental right of the citizen. But what kind of authorities should recognize, guarantee and protect this fundamental right? Digital commons include resources created and shared within a community of variable dimensions and interests: these resources are generally managed in common, according to a form that does not belong neither to private nor to public property. In addition, this organization takes to exploiting the resource within the community itself, and it does not address, at least as its primary objective, the market with profit-seeking objectives. The peculiar nature of digital commons is thus to ensure that members of their community have the right to access the resources, distribute and modify them: a right that is supported by the nature of digital goods that, unlike natural resources, are not exhaustible and can therefore be copied, shared, and processed without limiting the rights of others to use them¹¹⁹. This difference clearly differentiates them from the natural commons described by Ostrom and creates also some difficulties in applying clear rules and precise boundaries to the access to the resource itself (as was the case, for example, for the access to a grazing ground or a fishing zone).

To sum up the fundamental properties of digital commons, it may be useful to refer again to the following definition: *"...information and knowledge resources that are collectively created and owned or shared between or among a community and that tend to be non-excludable, that is, be (generally freely) available to third parties. Thus, they are oriented to favor use and reuse, rather than to exchange as a commodity. Additionally, the community of people building them can intervene in the governing of their interaction processes and of their shared resources"*¹²⁰. These principles have been applied in different areas of our lives, first of all in the field of scientific research, where the open access movement promoted open access to scientific resources as a key objective to be pursued in an effort to successfully spread the commons-oriented

¹¹⁸ In this regard, an important role is played by the free software movement, which is directed to make the software publicly available, favoring its free study and allowing to make changes to the resource.

¹¹⁹ In this sense, digital commons, since they gain more value as more people participate, are not exposed to the so-called *"tragedy of the commons"*, meaning they do not lose value as they are used or exploited (such as in the case of natural resources).

¹²⁰ Fuster Morell, M. (2010), *Dissertation: Governance of online creation communities: Provision of infrastructure for the building of digital commons*. p. 5.

approach in the digital society (we talk about open science in this regard)¹²¹. Another important example comes from the education sector, where free and open access is increasingly envisaged as an important means of improving the way that this fundamental educational function is being implemented.

From this backdrop the idea of cooperation, the role of the community and shared management can be applied to the organization of digital resources.

1.4 References

Bollier D. (2008). *Viral Spiral. How the Commoners Built a Digital Republic of Their Own*. New York, London, New Press.

Ciurcina M. (2017). Licenze di software libero ed altre licenze libere: codice genetico di beni comuni digitali. In: *DigitCult* (2, Iss. 1). 15–24.

Commissione Rodotà, (14 June 2007). Per la modifica delle norme del codice civile in materia di beni pubblici, proposal, Ministero della Giustizia.

Coriat B. (2013), “Property and Commons. The new issues of shared access and innovation”, International Seminar Paris

Digital Social Innovation Report (2015). Growing a digital social innovation ecosystem

Fuster Morell M. (2010). Dissertation: Governance of online creation communities: Provision of infrastructure for the building of digital commons

Hess C., Ostrom E. (eds.), 2006, “Understanding knowledge as a Commons. From Theory to Practice”, Cambridge, Massachusetts, The MIT Press

House of Commons, Science and Technology Committee (2016). The Big Data dilemma. fourth report of session 2015/16

Lessig L. (2004). *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York, Penguin Press

¹²¹ “Open access” can be a confusing term: in the context of a rivalrous, depletable natural resource, an open-access regime is not the same as a commons, because a commons does have rules, boundaries, sanctions against free riders, etc., to govern the resource. However, in the case of an infinite, non-rivalrous resource like information, which can be copied and distributed at virtually no cost, an open-access regime does not result in overexploitation of the resource. For this reason, open access in an Internet context is often conflated with the commons.

Lessig L. (2001). *The future of ideas: the fate of the commons in a connected world*. Random House.

Matias, J. N. (2015). *The Tragedy of the Digital Commons*. In: *The Atlantic*

Ostrom E. (1990). *Governing the Commons: the Evolution of Institutions for Collective Actions*. Cambridge University Press

Ostrom E., 8 December 2009, "Beyond Markets and States: polycentric governance of complex economic systems", Nobel Prize Lecture.

Stalder, F. (2010). *Digital Commons: a dictionary entry*. In: Hart, K., Laville, J.-L., Cattani, A. D. (eds) (2010). *The Human Economy: A World Citizen's Guide*. Cambridge, UK, Polity Press, pp. 313-324

Stallmann R. (2009). *Why Open Source misses the point of Free Software*

Vercellone C., Bria F., Fumagalli A., Gentilucci E., Giuliani A., Griziotti G., Vattimo P., Armstrong K. (30 April 2015). *Managing the commons in the knowledge economy*. Available at https://www.nesta.org.uk/sites/default/files/d-cent_managing_the_commons_in_the_knowledge_economy.pdf

Wemheuer-Vogelaar W. (2013). *Governing a Knowledge Commons: The Influence of Institutional Design on the Performance of Open Access Repositories*. Center of Global Politics, Berlin.

Annex B: Taxonomy

Term	Definition	Reference	Legal Domain
Acceptance	<p>(1) A statement made by or other conduct of the offeree indicating assent to an offer is an acceptance. Silence or inactivity does not in itself amount to acceptance.</p> <p>(2) An acceptance of an offer becomes effective when the indication of assent reaches the offeror.</p> <p>(3) However, if, by virtue of the offer or as a result of practices which the parties have established between themselves or of usage, the offeree may indicate assent by performing an act without notice to the offeror, the acceptance is effective when the act is performed.</p>	Art. 2.1.6, Unidroit Principles of International Commercial Contracts	CONTRACT LAW
Acceptor	who issues the acceptance		CONTRACT LAW
Agreement	A contract may be concluded either by the acceptance of an offer or by conduct of the parties that is sufficient to show agreement.	Art. 2.1.1, Unidroit Principles of International Commercial Contracts	CONTRACT LAW
Offer	A proposal for	Art. 2.1.2, Unidroit	CONTRACT LAW

	concluding a contract constitutes an offer if it is sufficiently definite and indicates the intention of the offeror to be bound in case of acceptance.	Principles of International Commercial Contracts	
Offeror	who issues the offer		CONTRACT LAW
Party	parties of an agreement (offerer or acceptor)		CONTRACT LAW
Work	every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression, such as books, pamphlets and other writings; lectures, addresses, sermons and other works of the same nature; dramatic or dramatic-musical works; choreographic works and entertainments in dumb show; musical compositions with or without words; cinematographic works to which are assimilated works expressed by a process analogous to cinematography; works of drawing, painting, architecture, sculpture, engraving and lithography; photographic works to which are assimilated works expressed by a process analogous to photography; works of applied art; illustrations, maps, plans, sketches and three-dimensional works relative to geography, topography, architecture or science; software and databases..	Art. 2, Convention of Berne	IP
Author	the creator of a work.	Art. 2, Berne Convention	IP
Copyright	The economic rights in the work and the moral rights of the author. The economic rights are rights which are limited in time and which		IP

	may be transferred by the author. They include the right to authorize the reproduction, the communication to the public and the distribution of the work.		
Copyright	legal concept giving the creator of an original work exclusive rights to it, usually for a limited time.		IP
Sui Generis Right on database	The rights given to the database maker to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.	Art. 7, art. 11, Dir. 96/9/EC	IP
License Agreement	The contract or other legal act under which the owner of an intellectual property right ('licensor') gives permission to another individual or entity ('licensee') to use the rights for a period of time and within defined territory.		IP
Owner of IPRs	The person or entity holding rights on a work or on other entity protected by IPRs.		IP
IPRs	Copyright, Sui Generis right on database, related rights, trademarks, geographical indications, industrial designs, patents, plant varieties, layout-designs of integrated circuits, and trade secrets.		IP
Anonymisation	is a technique applied to personal data in order to achieve irreversible de-identification. Therefore, the personal data must have been collected and processed in compliance with the applicable	Recital 26, GDPR	PRIVACY

	legislation on the retention of data in an identifiable format.		
consent (of the data subject)	means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her	Art. 4 (11) GDPR	PRIVACY
data controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;	Art. 4 (7) GDPR	PRIVACY
data minimization	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	Art. 5 (1.C) GDPR	PRIVACY
data processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	Art. 4 (2) GDPR	PRIVACY

data processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Art. 4 (8) GDPR	PRIVACY
data recipient	means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.	Art. 4 (9) GDPR	PRIVACY
data storage limitation	personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed	Art. 5(1), point e. GDPR	PRIVACY
data subject	an identified or identifiable natural person on whom data are referred	Art. 4.(1) GDPR	PRIVACY
identifiable natural person	is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	Art. 4 (1), GDPR	PRIVACY
personal data	any information relating to a data subject	Art. 4.(1) GDPR	PRIVACY
Pseudonymisation	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and	Art. 4 (5) GDPR, Opinion 05/2014 on Anonymisation Techniques	PRIVACY

	<p>organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.</p> <p>Pseudonymisation reduces the linkability of a dataset with the original identity of a data subject; as such, it is a useful security measure but not a method of anonymisation.</p>		
sensitive data	<p>special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.</p>	Art. 9 (1), GDPR	PRIVACY
third party	<p>means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data</p>	Art. 4 (10) GDPR	PRIVACY

Annex C: Bibliography

1. Digital Commons

Bollier, D. (2008). *Viral Spiral. How the Commoners Built a Digital Republic of Their Own*. New York, London, New Press.

Ciurcina, M. (2017). Licenze di software libero ed altre licenze libere: codice genetico di beni comuni digitali, *DigitCult (2)* 1, 15–24

Commissione Rodotà (14 June 2007). Per la modifica delle norme del codice civile in materia di beni pubblici. Proposal, Ministero della Giustizia

Coriat, B.(2013). Property and Commons. The new issues of shared access and innovation, International Seminar Paris

Digital Social Innovation Report (2015). Growing a digital social innovation ecosystem

Fuster Morell, M. (2010). Dissertation: Governance of online creation communities: Provision of infrastructure for the building of digital commons

Hess, C., Ostrom, E. (eds) (2006). *Understanding knowledge as a Commons. From Theory to Practice*. Cambridge, Massachusetts, The MIT Press

House of Commons, Science and Technology Committee (2016). *The Big Data dilemma*. Fourth report of session 2015/16.

Lessig, L. (2001). *The future of ideas: the fate of the commons in a connected world*. Random House

Lessig, L. (2004). *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York, Penguin Press

Matias, J. N. (2015). *The Tragedy of the Digital Commons*. *The Atlantic*

Ostrom, E. (1990). *Governing the Commons: the Evolution of Institutions for Collective Actions*. Cambridge University Press

Ostrom, E. (8 December 2009). Beyond Markets and States: polycentric governance of complex economic systems. Nobel Prize Lecture

Stalder, F. (2010). Digital Commons: a dictionary entry. In: Hart, K., Laville, J-L., Cattani, A.D. (eds). *The Human Economy: A World Citizen's Guide*. Cambridge, UK, Polity Press, pp. 313-324

Stallmann, R. (2009). Why Open Source misses the point of Free Software

Vercellone, C., et Al. (2015). Managing the commons in the knowledge economy, D-CENT project, European Commission. https://www.nesta.org.uk/sites/default/files/d-cent_managing_the_commons_in_the_knowledge_economy.pdf

Wemheuer-Vogelaar, W. (2013). Governing a Knowledge Commons: The Influence of Institutional Design on the Performance of Open Access Repositories. Center of Global Politics, Berlin

2. Legal aspects of Blockchain and Distributed Decentralized Architectures

Abramowicz, M. (2015). Peer-to-Peer Law, Built on Bitcoin. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2573788>

Arruñada, B. (2017). Blockchain's Struggle To Deliver Impersonal Exchange. *Economics Working Paper Series. Working Paper No. 1549*, Universitat Pompeu Fabra de Barcelona

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain - The Gateway to trust-free cryptographic Transactions. In *Twenty-Fourth European Conference on Information Systems (ECIS)* (pp. 1–14)

Boucher P. (2017). How blockchain technology could change our lives. European Parliamentary Research Service, Scientific Foresight Unit (STOA)

Boullier, D. (2016). Cosmopolitical composition of distributed architectures. *First Monday*, 21(12). <https://doi.org/10.5210/fm.v21i12.7128>

Buterin V., The Meaning of Decentralization, MEDIUM (February 6, 2017), available at <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274#.oz2xb0yxx>

Champagne P. (2012). The book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto. LLC e53 Publishing

De Filippi, P., Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*, 21(12). <https://doi.org/10.5210/fm.v21i12.7113>

Deloitte - *Blockchain Enigma. Paradox. Opportunity*

Drescher D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Ed. A Press

Dulong de Rosnay M. (2016). Peer to party: Occupy the law. *First Monday*, 21(12). <http://dx.doi.org/10.5210/fm.v21i12.7117>

Dulong de Rosnay M. (2015). Peer-to-peer as a design principle for law: distribute the law. *Journal of Peer Production*, (Issue 6: Disruption and the Law), 1–9. Available at: <http://peerproduction.net/issues/issue-6-disruption-and-the-law/peer-reviewed-articles/peer-to-peer-as-a-design-principle-for-law-distribute-the-law/>

Dupont, Q., & Maurer, B. (2015). Ledgers and Law in the Blockchain. *Kings Review*, (23rd June), 1–15

ESMA (2006). *The Distributed Ledger Technology Applied to Securities Markets*. In: European Securities and Markets Authority

Grigg., I. (2004). The Ricardian Contract. In *Proceedings of the First IEEE International Workshop on Electronic Contracting*. IEEE. Available at: http://iang.org/papers/ricardian_contract.html

Iansiti M., Lakhani K. R. (2017). The truth about blockchain. In: *Harvard Business Review*, Issue January February 2017

Karanasiou A.P. (2016). Law encoded: Towards a free speech policy model based on decentralized architectures. In: *First Monday* 21 (12). Available at <http://dx.doi.org/10.5210/fm.v21i12.7118>

Kypriotaki, K., Zamani, E., & Giaglis, G. (2015). From Bitcoin to Decentralized Autonomous Corporations - Extending the Application Scope of Decentralized Peer-to-Peer Networks and Blockchains. In *Proceedings of the 17th International Conference on Enterprise Information Systems* (pp. 284–290). SCITEPRESS - Science and Technology Publications

Reijers, W., & Coeckelbergh, M. (2016). The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies. In: *Philosophy & Technology*. <https://doi.org/10.1007/s13347-016-0239-x>

Swan M., *Blueprint for a new economy* (2015)

Wall E., Malm G., (2016). Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository. Department of Electrical and Information Technology,

Faculty of Engineering, LTH, Lund University

Werbach, K. D. (2018, forthcoming). Trust, But Verify: Why the Blockchain Needs the Law. In Berkeley Technology Law Journal

Wright, A., De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network*, 4-22. Retrieved from <http://papers.ssrn.com/abstract=2580664>

3. IPRs & Licensing

Baarbé J., Blom M., de Beer J. (2017). A Data Commons for Food Security. Working Paper 7 IASC 2017. Conference Paper Published: June 20, 2017. Open AIR

Bain, M. (2010). Software Interactions and the GNU General Public License. *International Free and Open Source Software Law Review* 2-2. Accessed June 15, 2017. <http://www.ifosslr.org/ifosslr/article/view/44>

De Miguel Asensio P., (2012). Internet Intermediaries and the Law Applicable to Intellectual Property Infringements. *JIPITEC, Vol. 3*

Edwards L., Moss G., Karvelyte K. (2017). Living With(in) Copyright Law: What is it, how does it work, how could it change? Project Report. CREATE Working Paper 2017/10. DOI: 10.5281/zenodo.583247

Erickson, K. (2014). User illusion: ideological construction of 'user-generated content' in the EC consultation on copyright. *Internet Policy Review*, 3(4), 1-19. <https://doi.org/10.14763/2014.4.331>

Fontana, Richard, and Kuhn, Bradley M., and Moglen, Eben, and Norwood, Matthew, and Ravicher, Daniel B., and Sandler, Karen, and Vasile, James, and Williamson, Aaron. A Legal Issues Primer for Open Source and Free Software Projects, Accessed May 16, 2017. <http://softwarefreedom.org/resources/2008/foss-primer.pdf>

Hemel, Armijn, and Coughlan, Shane. Practical GPL Compliance. San Francisco, CA: Linux Foundation, 2017

Jakob SF (2014). A Qualitative Study on the Adoption of Copyright Assignment Agreements (CAA) and Copyright License Agreements (CLA) within Selected FOSS Projects. *JIPITEC*, Vol. 5

Jurčys, P. (2012). International Jurisdiction in Intellectual Property Disputes. *JIPITEC*, Vol. 3

Kim, M. (2007). The creative commons and copyright protection in the digital era: Uses of creative commons licenses. *Journal of Computer-Mediated Communication*, 13(1), 187–209. <https://doi.org/10.1111/j.1083-6101.2007.00392.x>

Kuhn, Bradley M., and Sebros, Anthony K. Jr., and Gingerich, Denver, and Free Software Foundation, Inc., and Software Freedom Law Center. Copyleft and the GNU General Public License: A Comprehensive Tutorial and Guide, Accessed May 16, 2017. <https://copyleft.org/guide/>

Kur A., Dreier T. (2013). European intellectual property law. Text, cases and materials. Edward Elgar Ed.

Lee Y. H., Laidlaw E., Copyright and Freedom of Expression : A Literature Review". CREATE Working Paper 2015/04 (May 2014) DOI: 10.5281/zenodo.18132

Margoni, Thomas. "Not for Designers: On the Inadequacies of EU Design Law and How to Fix It" *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 4-3 (2013). 225-248. Accessed May 16, 2017. <http://www.jipitec.eu/issues/jipitec-4-3-2013/3845/margoni.pdf>

Meeker, Heather, Open source for business. A practical guide to open source licensing. North Charleston SC: Createspace Independent Publishing Platform, 2017

Metzger, Axel. Free and Open Source Software (FOSS) and other Alternative License Models: A Comparative Analysis. Switzerland: Springer International, 2016

Rosati E. (2016). Why a reform of hosting providers' safe harbour is unnecessary under EU copyright law. *European Intellectual Property Review*, Vol. 38, Issue 11, pp. 668-676, 2016

Rosen, Lawrence. Open source licensing: software freedom and intellectual property law. Upper Saddle River, NJ: Prentice Hall Professional Technical Reference, 2005

Schmitz, P.-E. (2013). The European Union Public Licence (EURL). *International Free and Open Source Software Law Review*, 5, 121–136. <https://doi.org/10.5033/ifosslr.v5i2.9>

Van den Brande, Y., et Al. (2011). The International Free and Open Source Software Law Book. Open Source Press GmbH, 2011. Accessed May 16, 2017. <http://ifosslawbook.org>

Vaver D., Sirinelli P. (2002). Principles of Copyright Law – Cases and Materials. WIPO

Weber, Steven. The Success of Open Source. Cambridge, Massachusetts: Harvard University, 2004

Zech, H. (2015). Information as Property. *JIPITEC*, Vol. 6

3.1 IPRs & Blockchain

Cawrey, D. (2014). How Bitcoin's Technology Could Revolutionize Intellectual Property Rights. Available online at: <http://www.coindesk.com/how-block-chain-technology-is-working-to-transform-intellectual-property/>

Swan, M. (2015). Blueprint for a new economy. O'Reilly Media, Inc. (pp. 1–30). Available at <https://doi.org/10.1017/CBO9781107415324.004>

3.2 Legislation

3.2.1 EU legislation

Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products; see <http://data.europa.eu/eli/dir/1987/54/oj>

Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission; see <http://data.europa.eu/eli/dir/1993/83/oj>.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases; see <http://data.europa.eu/eli/dir/1996/9/oj>.

Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the patentability of biotechnological inventions; see <http://data.europa.eu/eli/dir/1998/44/oj>

Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs; see <http://data.europa.eu/eli/dir/1998/71/oj>

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; see <http://data.europa.eu/eli/dir/2001/29/oj>

Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art ("Resale Right Directive"); see <http://data.europa.eu/eli/dir/2001/84/oj>.

Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs; see <http://data.europa.eu/eli/reg/2002/6/2013-07-01>

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights; see <http://data.europa.eu/eli/dir/2004/48/corrigendum/2004-06-02/oj>.

Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property; see <http://data.europa.eu/eli/dir/2006/115/oj>

Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights; see <http://data.europa.eu/eli/dir/2006/116/oj>.

Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trademarks; see <http://data.europa.eu/eli/dir/2008/95/oj>

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs; see <http://data.europa.eu/eli/dir/2009/24/oj>.

Directive 2011/77/EU of the European Parliament and of the Council of 27 September 2011 amending Directive 2006/116/EC on the term of protection of copyright and certain related rights; see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:265:0001:0005:EN:PDF>.

Directive 2012/28/EU of the European Parliament and of the Council of 25 October 2012 on certain permitted uses of orphan works; see <http://data.europa.eu/eli/dir/2012/28/oj>.

Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection; see <http://data.europa.eu/eli/reg/2012/1257/oj>

Council Regulation (EU) No 1260/2012 of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection with regard to the applicable translation arrangements; see <http://data.europa.eu/eli/reg/2012/1260/oj>

Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market; see <http://data.europa.eu/eli/dir/2014/26/oj>.

Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks; see <http://data.europa.eu/eli/dir/2015/2436/oj>

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure; see <http://data.europa.eu/eli/dir/2016/943/oj>

Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark; see <http://data.europa.eu/eli/reg/2017/1001/oj>

3.2.2 International Treaties

Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886

Universal Copyright Convention (UCC), Geneva, 6 September 1952

Patent Cooperation Treaty of June 19, 1970

Convention on the Grant of European Patents of 5 October 1973 (European Patent Convention or EPC)

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) signed in Marrakesh, Morocco on April 15th 1994

WIPO Copyright Treaty (WCT), adopted in Geneva on December 20, 1996; see http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=295166

WIPO Performances and Phonograms Treaty (WPPT), adopted in Geneva on December 20, 1996; see http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=295578

Agreement on a Unified Patent Court (UPC), EU Document 16351/12; see <https://www.unified-patent-court.org/sites/default/files/upc-agreement.pdf>

3.3 Opinions, recommendations and standards

ARTICLE 29 Data Protection Working Party, Working document on data protection issues related to intellectual property rights, adopted on January 18, 2005 (WP 104)

4. Privacy and data protection

Ambrose, M. L., & Ausloos, J. (2013). The Right to Be Forgotten Across the Pond. *Journal of Information Policy*, 3, 1–23. <https://doi.org/10.5325/jinfopoli.3.2013.0001>

Borking, J. J., & Raab, C. (2001). Laws, PETs and other technologies for privacy protection. *Journal of Information, Law and Technology*, 1(February), 1–14

Cavoukian A. (2010). Privacy by Design: the definitive workshop. In *Identity in the information society* (3) 2, pp. 247-251

Cavoukian A., Jonas J. (2012). Privacy by Design in the Age of Big Data. Information and Privacy Commissioner of Ontario

Colesky M., Hoepman J-H., Hillen C. (2016). A critical analysis of Privacy Design Strategies, 2016 IEEE Security and Privacy Workshops, pp. 33-40

Danezis, G. (2007). Introduction to privacy technology, Katholieke Universiteit Leuven, Computer Security and Industrial Cryptography (COSIC) Res. Available from: http://research.microsoft.com/enus/um/people/gdane/talks/Privacy_Technology_cosic.pdf

Dwork, C. (2006). Differential privacy. In *Automata, languages and programming*, pages 1–12. Springer

Floridi L. (ed.) (2014). Protection of Information and the Right to Privacy - A new Equilibrium?. Dordrecht, Springer

Floridi L. (2016). Four challenges for a theory of informational privacy. In *Ethics and Information Technology* (8) 3 pp. 109-119

Geib C. (2016). From infringement to exception: why the rules on data mining in Europe need to change. CREATE Working Paper 2016/07

Green B. , Cunningham G., Ekblaw A., Kominers P., Linzer A., Crawford S. (2015). Open data privacy: A risk-benefit, process-oriented approach to sharing and protecting municipal data. Berkman Klein Center for Internet & Society

Gutwirth S., Leenes R., De Hert P (eds.) (2012). *European Data Protection: In Good Health?* Dordrecht, Springer

Gutwirth S., Leenes R., De Hert P. (eds.) (2014). *Reforming European Data Protection*. Springer

Hoepman, J-H. (2014). Privacy Design Strategies, IFIP TC11 29th Int. Conf. on Information Security (IFIP SEC 2014), pp. 446-459

Janal, R. (2017). Data Portability - A Tale of Two Concepts. *JIPITEC*, Vol. 8

Kerber, W. (2016). Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection (April 26, 2016). *Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil* (GRUR Int) 2016, 639-647. Available at: <http://dx.doi.org/10.2139/ssrn.2770479>

Koops B-J., Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law'. In: *International Review of Law, Computers & Technology* (28), 2, pp. 159-171

Krebs, D. (2013). " Privacy by Design ": Nice-to-have or a Necessary Principle of Data Protection Law?. *JIPITEC*, 4, 20

Lueks W., Everts M. H., Hoepman J. H. (2016). Revocable privacy: Principles, use cases, and technologies. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* Vol. 9484, Issue 318424, pp. 124-143

Pagallo, U. (2012a). Cracking down on autonomy: three challenges to design in IT Law, *Ethics Information Technology* (14), pp. 319-328

Pagallo, U. (2012b). On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In Gutwirth S., Leenes R., De Hert P., *European Data Protection: In Good Health?*. pp. 331 – 346

Pagallo U., Bassi E. (2013). Open data protection: challenges, perspectives and tools for the reuse of PSI. In: M. Hildebrandt, K. O'Hara, M. Waidner (eds.). *Digital Enlightenment Yearbook 2013*. Amsterdam. los. pp. 179-189

Pfitzmann, A., & Hansen, M. (2001). Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology. *Designing Privacy Enhancing Technologies, 2009*, 1–9. <https://doi.org/10.1.1.153.6354>

Reynolds S. et Alii (2015). Review of the EU copyright framework. The implementation, application and effects of the "InfoSoc" Directive (2001/29/EC) and of its related instruments. EPRS

Solove D.J. (2013). Privacy, Self-management and the Consent Paradox. In: *Harvard Law Review* (126) 7, pp. 1880-1903

Spindler G., Schmechel P. (2016). Personal Data and Encryption in the European General Data Protection Regulation. *JIPITEC*, Vol. 7

Tamò A., George D. (2014). Oblivion, Erasure and Forgetting in the Digital Age. *JIPITEC*, Vol. 5

Van Alsenoy, B. (2017). Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation. *JIPITEC*, Vol. 7

Van der Sloot, B. (2015). Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe. *JIPITEC*, Vol. 6

Voss W. G., Castets-Renard, C. (2016). Proposal for an International Taxonomy on the Various Forms of the 'Right to Be Forgotten': A Study on the Convergence of Norms (June 26, 2016). 14 *Colorado Technology Law Journal* 281 (2016) (Issue 14.2) (pp. 281-344). Available at SSRN: <https://ssrn.com/abstract=2800742>

Wright D., De Hert P. (eds.) (2012). *Privacy Impact Assessment*. Dordrecht, Springer

4.1 Privacy & Blockchain

Berberich M., Steiner M. (2016). Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?. *EDPL* (3), pp. 422-426

Buterin V. (2016). Privacy on the Blockchain. Online available at: <https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/>

De Filippi P. (2016). The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies. *Journal of Peer Production*, Issue n.7: Alternative Internets . Available at SSRN: <https://ssrn.com/abstract=2852689>

Peeters R., Pulls T. (2015). *Regaining the end-users' trust with transparency-enhancing tools*. In Amsterdam Privacy Conference 2015

Smith J., Tennison J., Wells P., Fawcett J., Harrison S. (2016). *Applying blockchain technology in global data infrastructure*. Ed. Anna Scott, ODI Open Data Institute

Zyskind G., Nathan O., Pentland A. (2015). *Decentralizing privacy: Using blockchain to protect personal data*. Security and Privacy Workshops (SPW), 2015 IEEE

4.2 Legislation

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive)

REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

4.3 Recommendations and standards

ARTICLE 29 Data Protection Working Party, Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector (WP 239)

ARTICLE 29 Data Protection Working Party, Statement on the 2016 action plan for the implementation of the General Data Protection Regulation , adopted on 2 February 2016 (WP 236)

ARTICLE 29 Data Protection Working Party, Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, adopted on 16 September 2014 (WP 221)

ARTICLE 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216)

ARTICLE 29 Data Protection Working Party, Opinion 03/2014 on Personal Data Breach Notification (WP 213)

ARTICLE 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203)

ARTICLE 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability (WP 173)

ARTICLE 29 Data Protection Working Party Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169)

ARTICLE 29 Data Protection Working Party & Working Party on Police and Justice, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP 168)

ARTICLE 29 Data Protection Working Party, Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) (WP 159)

ARTICLE 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data (WP 136)

ARTICLE 29 Data Protection Working Party, Working document on data protection issues related to intellectual property rights, adopted on January 18, 2005 (WP 104)

ARTICLE 29 Data Protection Working Party, Opinion 7/2003 on the re-use of public sector information and the protection of personal data (WP 83)

5. Smart Contracts

AA.VV., Smart Contracts : Coding the fine print. A legal and regulatory guide (2016). Norton Rose Fulbright

Bourque, S., Tsui, S. F. L. (2014). A Lawyer's Introduction to Smart Contracts. In *Scientia Nobilitat - Reviewed Legal Studies*, pp. 4–23

Clack C. D., Bakshi V. A., Braine L. (2016). Smart Contract Templates: essential requirements and design options. Available at: <http://arxiv.org/abs/1612.04496>

Felten E. (2017). Smart Contracts: Neither Smart nor Contracts?. In: *Freedom to Tinker: research and expert commentary on digital technologies in public life*. Available at <https://freedom-to-tinker.com/2017/02/20/smart-contracts-neither-smart-not-contracts/>

Frantz C K, Nowostawski M., From institutions to code: Towards automated generation of smart contracts (Conference Paper), Proceedings - IEEE 1st International Workshops on Foundations and Applications of Self-Systems, FAS-W 201616 December 2016, Article number 7789470, pp. 210-215

Glatz F. (2014). What are Smart Contracts? In search of a consensus. Available online at: <https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad>

Idelberger F., Governatori G., Riveret R., Sartor G. (2016). Evaluation of Logic-Based Smart Contracts for Blockchain Systems. In: Alferes J., Bertossi L., Governatori G., Fodor P., Roman D. (eds) *Rule Technologies. Research, Tools, and Applications. RuleML 2016. Lecture Notes in Computer Science*, vol 9718. Springer

Lauslahti, K., Mattila, J., Seppälä, T. (2017). *Smart Contracts – How will Blockchain Technology Affect Contractual Practices ?* ETLA Reports (Vol. 68, pp. 1–26)

Lesaege C. (2016). Decentralized Arbitration Court. White Paper

Levy, K. E. C. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science, Technology, and Society*, 3, 1. Available at <https://doi.org/10.17351/ests2017.107>

O'Shields, R. (2017). Smart Contracts: Legal Agreements for the Blockchain, 21 N.C. Banking Inst. 177. Available at: <http://scholarship.law.unc.edu/ncbi/vol21/iss1/11>

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2(9). <https://doi.org/10.5210/fm.v2i9.548>

Von Haller Groenbaek M. (2016). Blockchain 2.0, Smart Contracts and Legal Challenges. Available at: <https://www.scl.org/articles/3668-blockchain-2-0-smart-contracts-and-legal-challenges>

Wall E., Malm G., (2016) .Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository. Department of Electrical and Information Technology, Faculty of Engineering, LTH, Lund University

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network*, 4–22.